POLICING ILLEGAL DRUG AND WILDLIFE TRADES – THE ROLE OF THE POLICE, LEGAL ONLINE PLATFORMS, PRIVATE ORGANISATIONS AND INDIVIDUALS, AND CYBERCRIMINAL TRADERS

Lonie Sebagh

A thesis submitted for the degree of Doctor of Philosophy

Department of Sociology

St Cross College, University of Oxford

Trinity Term 2021

75,000 words (excluding References and Appendices)

POLICING ILLEGAL DRUG AND WILDLIFE TRADES – THE ROLE OF THE POLICE, LEGAL ONLINE PLATFORMS, PRIVATE ORGANISATIONS AND INDIVIDUALS, AND CYBERCRIMINAL TRADERS

Abstract

This thesis explores the actors and activities involved in the policing of online illegal drug and wildlife trades on the Darknet and surface web. As the role of policing evolves due to advances in technology, the blurring of national boundaries, the increasing knowledge and skills of other actors, and the growing volume and value of these trades, more research is required about who and what is involved in this endeavour to increase its efficiency.

Policing has been argued to take place in a network, where various actors come together to perform operations (Dupont, 2004). One of the most recent policing classifications is Button (2019)'s policing taxonomy which involves technological components. This thesis designs its own policing framework and tests the relevance of Button (2019)'s model in the context of online illegal drug and wildlife trades. Beyond the Police which possess powers of search and arrest to protect citizens, legal online platforms have created trading policies and are monitoring and punishing misconduct on their sites to preserve their legality and reputation. Organisations and individuals in the private sector, non-profits, and academia have been gathering, analysing, and sharing data and expertise to help Police investigations and inform the public. Cybercriminal traders have also taken advantage of others for their own financial gain and consequently decreased trust on Darknet markets, as well as unintentionally providing the Police with ways to disrupt their markets from the inside.

This exploratory research used mixed social science methods to gather complimentary quantitative and qualitative insights. Semi-structured interviews were performed with 20 experts in Police agencies, legal platforms, for-profit and non-profit organisations, and academia. The content of 200 Police and private organisation reports, news articles, blog posts, and legal platforms' trading policies was analysed. A pilot laboratory experiment also tested the behaviour of 138 participants following trust-related policing interventions in a fictitious online marketplace.

This thesis contributes to the fields of sociology and (cyber)criminology by designing a new cyber policing classification based on the policing of online illegal drug and wildlife trades and by formulating the first 'policing script' summarising the activities various policing actors perform in this context, when, with whom, and how they complement each other.

Acknowledgements

First, I would like to express my deepest gratitude to the experts who all so kindly agreed to talk to me and share their experiences and opinions for this research. This project would not have been complete without their insights. I also appreciate the hundreds of students who gave their time to participate in our novel social experiment and the Centre for Experimental Social Sciences for helping make it a reality.

I am thankful to my supervisors, Jonathan Lusthaus and Federico Varese, for lighting the way into a field I previously knew nothing about, suggesting ways to improve my project, encouraging me to write early on, which made the write up process a lot less stressful, and making me believe in my ability as a researcher. I would also like to thank Edoardo Gallo and Sean Sirur for their support with the experimental part of my research.

I am also grateful to my Transfer and Confirmation examiners, Michael Biggs, David Kirk, and Joss Wright, for their feedback and encouragement during these milestones, and to journal reviewers and conference/talk attendees at home and abroad for asking insightful questions and providing great comments to help my research evolve over the years.

I would also like to thank my Master's thesis supervisor, Richard Woodward, who got me interested in doing academic research, and my previous manager Eldo Mabiala, who made me discover the world of cyber security. Both of their influences have led me to pursue a PhD and stand where I am today.

The past four years in Oxford would not have been the same if I hadn't shared them with colleagues at the Centre for Doctoral Training in Cyber Security, St Cross College, and the Department of Sociology. I have cherished the academic, professional, and personal connections I have made with each of them along the way.

I am thankful for all the training, support, and resources the Centre for Doctoral Training in Cyber Security has provided us with, from specialised courses to game nights, Christmas parties, and great company, ensuring our doctoral journeys were not lonely ones.

A special thank you also goes to the St Cross College leadership team for entrusting me to become a student leader in more ways than one, to Seth Stadel for being the best co-Junior Dean I could have wished for, to the College staff for being amazing colleagues and some of the most caring people I have ever worked alongside, and the College kitchen team for feeding me delicious meals during long research days.

Finally, I am deeply grateful to my beloved family and friends near and far for their continuous encouragement and support during this journey. To my parents and brother who celebrated my highs and always provided light and reassurance during my lows, I am forever indebted to them. To my academic family, Adam and Cal, for their generosity, support, and many snack breaks. To my inspiration, Julie, for always believing in me and encouraging me to the best version of myself. To my cyber partners in crime, Klaudia and Selina, for our lunches, teas, and catch ups. And to Fede for sharing this doctoral journey with me from the beginning.

Table of contents

List of Figures

Chapter 5 – Legal Online Platforms

Chapter 6 – Private Organisations and Individuals

Chapter 7 – Cybercriminal traders

Figure 7.16: Frequency of tokens sent during the first (top) and second (bottom) trust games in slander sessions

Figure 7.17: Frequency of tokens sent back during the first (top) and second (bottom) trust games in slander sessions

Figure 7.18: Frequency of tokens sent during the first (top) and second (bottom) trust games in Sybil sessions

Figure 7.19: Frequency of tokens sent back during the first (top) and second (bottom) trust games in Sybil sessions

List of Tables

Chapter 2 – Literature Review

Chapter 3 – Methods

Chapter 7 – Cybercriminal traders

Chapter 8 - Discussion

1 Introduction

This introduction aims to provide context for the author's research and signpost this thesis' structure.

1.1 Research context and significance

Although online drug trading volumes are still considerably lower than their offline counterparts, drugs - chemical agents that alter biochemical and physiological processes (UNODC, 2021b) - and related products, now constitute two thirds of all traded products on Darknet markets (EMCDDA and Europol, 2017a). These are online marketplaces on an encrypted part of the Internet only accessible through specific software, which enable the sale of illegal goods and services online (Décary-Hétu and Giommoni, 2016). Darknet markets are increasingly privileged over offline ones for illegal trade, due to the increased range of products, reduced prices, and protection from violence and threats they offer to buyers, and the anonymity and financial opportunities they provide to vendors and administrators (Van Buskirk et al., 2014; Barratt et al., 2016; Décary-Hétu and Giommoni, 2016; United States Court of Appeals for the Second Circuit, 2016). The Police have therefore been tasked with disrupting these Darknet markets in order to reduce illegal drug trade and has made this threat a priority (Europol, 2019g). Two of the methods most employed by the Police have been to take down Darknet markets' digital infrastructure, by closing individual sites down, and to arrest their administrators, as was the highly publicised case for Ross Ulbricht and the Silk Road in 2013 (Van Buskirk et al., 2014; Bilton, 2018). Responses to these interventions have been analysed and these techniques have been criticised for leading to the displacement of cybercriminal trade at later times, in other marketplaces, or through other traders (Yip, Webber, et al., 2013; Van Buskirk et al., 2014; Décary-Hétu and Giommoni, 2016; Hutchings et al., 2016; Paquet-Clouston et al., 2017; Van Buskirk et al., 2017; Ladegaard, 2018). Other disruption methods used more recently include leaving false feedback to vendors and making fictitious reputable accounts default on their trades (Décary-Hétu and Dupont, 2013; Yip et al., 2013b; Hutchings and Holt, 2017; Paquet-Clouston et al., 2018), to instil mistrust between traders. These operations simulate scamming and exit scamming behaviours exhibited by cybercriminal traders themselves in these marketplaces, which have been shown to decrease cooperation and trust among traders (Soska and Christin, 2015).

Illegal drug trades are also increasingly happening on the surface web, sites indexed on and accessible through common search engines, upon which many of the above policing interventions cannot be conducted as they would perturb legal trades. Over the last few years, numerous news and academic articles have pointed to increasing amounts of these trades on legitimate websites and social media platforms. Indeed, these legal platforms are more broadly accessible and convenient than Darknet markets (Babb, 2014; Thanki and Frederick, 2016; EMCDDA and Europol, 2019; Moyle et al., 2019), and easier to set up, as very few barriers are present on popular social media platforms. This is even the case for profiles that are created for visibly illegal online pharmacies which fail to be taken down (Mackey and Liang, 2013). These legal platforms therefore represent another enforcement challenge (Martin et al., 2018a). Considering these increased trades on their sites, Facebook, Twitter, and Google founded the group Tech Together to Fight the Opioid Crisis in 2018 alongside the Center for Safe Internet Pharmacies (CSIP, 2021b), aiming to reduce drug trade, raise awareness, and provide help to fight users' addictions (Facebook, 2018b). Such collaborations between legal online platforms and other organisations have therefore been utilised to ensure the legitimacy of these sites by removing illegal listings and blocking criminal users.

While illegal wildlife species and products are not widely available on Darknet markets (Harrison et al., 2016; Cugniere et al., 2019; Wright, 2019), non-profit organisations have also reported growing volumes of these trades on the surface web as part of their research. In fact, a recent trend has been observed according to which up to 80% of this online trade might now be happening on social media platforms (Krishnasamy and Stoner, 2016), freely and easily accessible by many across the world (IFAW, 2018a; WJC, 2018a; TRAFFIC, 2019). These alarming volumes of online illegal wildlife trade have led to the creation of the Coalition to End Wildlife Trafficking Online in 2018 involving trading, social media, and instant messaging sites, such as eBay, Etsy, Facebook, and Instagram. These legal online platforms came together to reduce illegal wildlife trade and to receive the support of individuals and organisations specialised in these issues (Coalition to End Wildlife Trafficking Online, 2020). Indeed, due to both the Police's and these sites' limited resources and capacity in the policing of online illegal drug and wildlife trades, there has been a need for other stakeholders to get involved in these policing efforts and to provide their expertise and skills to the groups at the forefront of this policing.

As knowledge about these policing processes are limited in the academic literature, this thesis aims to ascertain whether the range of actors and activities involved in policing online illegal drug and wildlife trades, on the Dark and surface webs, are common between both products.

Indeed, drugs and wildlife are similar in many respects. They can both be traded in natural and synthetic forms which require physical shipment, and they are extracted from their natural environments, manufactured to desired specifications, and smuggled across borders in similar ways and often by the same people (South and Wyatt, 2011; Lavorgna, 2014a, 2014b). Their high trading volumes and values (IFAW, 2007, 2014d; EMCDDA and Europol, 2017a, 2019) have given rise to opportunistic and financially-motived involvement by traders, including Organised Crime Groups. Many of these Groups got involved in drug trade in the 1970s and 1980s as it wasn't perceived as very risky and recently moved to wildlife products for similar reasons (South and Wyatt, 2011). Drugs and wildlife are mainly traded nationally despite production and poaching taking place far from demand countries (Interpol and IFAW, 2013; Dittus et al., 2018). They both also have deep impacts on national economies and security (Viollaz et al., 2018), including health and violence in consumer countries and corruption and destruction of the environment in source countries (South and Wyatt, 2011; Europol, 2012; IFAW, 2013).

However, one main difference remains between drugs and wildlife: the priority afforded to them as part of enforcement activities. Indeed, drugs were extended a priority policing status long before their sale began on the Internet, which is believed to have started in the early 1970s on online academic networks (The Economist, 2014), and they are the criminal product that has received the most attention related to its Internet-mediated trafficking (Lavorgna, 2014a). However, wildlife species and products are just starting to be referred to as a mild threat (Europol, 2017g) following years of lobbying from animal welfare organisations, and they have not yet been offered the same extensive Police commitment (South and Wyatt, 2011). We therefore have much to gain from researching both of these products as part of the same study, gathering complementary insights which might provide useful strategies for their future respective policing. It might initially seem that this strategy would only allow for a better understanding of the policing of online illegal wildlife trade following the more thoroughly studied illegal drug trade (South and Wyatt, 2011). However, it has been argued

that the war against drugs has gone on for decades and that the situation is currently at its worst (Collins and et al, 2020). While researchers in the Netflix series 'The business of drugs' aim to apply anti-terrorism strategies to the war on drugs (Collins and et al, 2020), methods used in the policing of online illegal wildlife trade could also be investigated and in turn offer insights about the policing of the evolving drug trade.

Online illegal drug and wildlife trades may currently only represent a small percentage of the entire trade in these products (Europol, 2021e; UNODC, 2021d), but their online components are growing rapidly. In fact, Darknet markets reached an all-time-high of $1.7bn in revenue in 2020 (Chainanalysis, 2021), as people relied on online trading more heavily during the COVID-19 pandemic. It is therefore paramount to develop an understanding of these policing processes now. Indeed, following these technological developments, many studies have reported on the range of cybercriminals involved in these trades, their profiles, motivations, processes, collaborators, and outcomes, but little to no research is available on the actors involved in the policing of these online trades.

Theories exist, however, about different kinds of policing involved in various other policing activities. Most relevantly, Button (2019)'s policing framework draws on previous theories, expands upon their limitations, and was recently updated to include the policing of technological realms. According to Button (2019), there are four categories of policing actors – 1) the State Police, 2) the Hybrid Police, 3) the Voluntary Police, and 4) the Private Security Industry – which exist on a continuum of public and private organisations involved in policing activities (see Chapter 2). While the first two categories relate to public enforcement efforts, both involving uniformed officers performing general duties and specialised agencies, the Voluntary Police refers to individuals and organisations which participate in policing while not mandated to do so, and the Private Security Industry pertains to individuals and organisations hired to conduct private security duties (Button, 2019). This classification can therefore be evaluated for the under-researched policing of online illegal drug and wildlife trades.

As specific policing frameworks have not yet been devised with regards to online illegal trade, this thesis aims to design its own classification in this cyber policing context and to test the suitability of Button (2019)'s framework in this cyber environment. This thesis also concludes by devising the first 'policing script' integrating findings about the various groups involved in

the policing of online illegal drug and wildlife trades. This script summarises the activities each group performs at each stage, deepening our understanding of this process and displaying areas for increased efficiency. This novel concept mirrors that of 'crime scripts' which have been used for decades to describe the conduct of crimes and their various stages, in order to identify where the Police and others could interfere to stop them most effectively (Cornish, 1994). Crime scripts have recently been applied to crimes conducted online (Hutchings and Holt, 2015; Leukfeldt et al., 2016b; Warren et al., 2017), and Lavorgna (2014a, 2014b) has specifically applied them in the case of online illegal drug and wildlife trades. In fact, when Dehghanniri and Borrion (2019) systematically reviewed 105 crime scripts designed between 1994 and 2018, they found that the category with the most original scripts was that of cybercrime, followed by corruption and fraud, robbery and theft, drugs offences, environmental crime, violent crime, and sexual offences. Scripting policing activities on the policing side of these cybercrimes could therefore bring a higher degree of understanding about these activities, as well as increased efficiency, as more policing groups could identify where their skills and resources are most needed.

This thesis therefore aims to answer questions about the actors and activities involved in the policing of online illegal drug and wildlife trades, whether they vary between both products, and how this type of policing can be more effective in the future.

The structure of this thesis leading up to the cyber policing framework and policing script is presented in the next section.

1.2 Thesis structure

This thesis follows the below monograph structure.

Following this Introduction, the Literature Review chapter will first provide some theoretical background about online illegal trade on Dark and surface markets, illegal drugs and wildlife species and products sold online, and the various operations conducted by the Police and others to disrupt these trades. The classification of policing section will then detail Button (2019)'s policing framework, one of the most recent policing taxonomies adapted to include the policing of cybercrime. This chapter will point to current gaps in our understanding of online illegal drug and wildlife trades policing, the different actors who come together to conduct these disruptions, and the activities they each perform.

The Methods chapter will describe the mixed social science methods used to gather complementary insights as part of this exploratory project. The researcher conducted 20 semi-structured interviews to gather qualitative insights from experts in the field about their roles in the policing of online illegal drug and wildlife trades. The researcher then performed content analysis to gather quantitative data about the frequency of specific expressions mentioned in 200 Police and other publications. This analysis also allowed for additional qualitative insights to be drawn about the policing operations referenced by certain organisations in specific ways and at specific times. Finally, the researcher organised a social laboratory experiment simulating a fictitious online marketplace where 138 participants' behaviours were observed following trust-related policing interventions.

Four empirical chapters will then be presented which evaluate the role of four different groups involved in the policing of online illegal drug and wildlife trades – the Police, legal online platforms, private organisations and individuals, and cybercriminal traders.

The first empirical chapter will explore the role of the Police. While the Police have conducted infrastructure takedowns, seizures, and arrests, often in collaboration and coordination with other agencies, to disrupt online illegal drug trade on the Darknet, its involvement in the policing of online illegal wildlife trade has been more restrained. Indeed, this trade is more prevalent on the surface web and support is therefore required from legitimate platforms responsible for maintaining the legality of their sites and removing any illegal content. The

Police also seek expertise from private organisations and individuals who specialise in online illegal drug and wildlife trade issues to provide them with relevant information and resources.

The second empirical chapter will then scrutinise the role of legal online platforms in the policing of online illegal drug and wildlife trades. Indeed, these platforms put in place trading policies on their sites to signal what trades are legal and accepted on their platforms with the support of private organisations' and individuals' expertise. These legal platforms then monitor these policies are abided by, identify any misconducts, and remove any criminal users or listings from their sites. While enabling trade is their main focus, security has therefore become a non-optional addition to their core activities.

The third empirical chapter will investigate the role of private organisations and individuals in different industries and sectors in the policing of online illegal drug and wildlife trades. Although their activities are less visible and understood than those of the Police, actors in private industry, non-profits, and academia are indispensable to these interventions. Indeed, private organisations and individuals possess specific knowledge and skills which the Police and legal online platforms require, giving them a prominent place in this type of policing despite this not always being their main area of activity.

Finally, the fourth empirical chapter will demonstrate that cybercriminal traders themselves, the people buying and selling products and services on Darknet markets, have a role to play in the policing of their own trades and marketplaces. Indeed, many scams and exit scams have been witnessed on Darknet markets, including vendors selling low-quality or non-existent products which buyers do not receive, or administrators closing down and exiting their Darknet market with all of the money held in escrow, leaving traders out of pocket. These behaviours have weakened these marketplaces, as traders' trust in one another decreased. The Police and other private individuals and organisations working to disrupt these trades have therefore reproduced this behaviour at scale to disrupt these marketplaces from the inside.

The Discussion chapter will then answer the general research questions stated in the following Literature review chapter. This thesis argues that Button (2019)'s policing classification does not entirely suit this thesis' cyber context and the researcher's framework

based on the four above policing groups better represents the policing of online illegal drug and wildlife trades. These findings are finally collated in a 'policing script' which improves our understanding of this particular policing context and suggests more efficient processes for these interventions to be performed. Indeed, the script will ideally help the actors involved in this process realise what policing activities they or others are better suited to and what they should rely on others for.

Finally, the Conclusion will summarise the answers to the overall thesis research questions and the contribution of this study to the fields of sociology and (cyber)criminology. It will also share policy recommendations for the Police and others participating in the policing of online illegal drug and wildlife trades, and suggest subsequent research that could be undertaken in the field to further increase the effectiveness of this collaborative policing.

The following chapter reviews the relevant academic literature underlying this thesis.

2 Literature Review

This chapter provides theoretical background about online illegal trade, illegal drug and wildlife species and products sold online, the various operations conducted by the Police and others to disrupt these trades, and the classification Button (2019) devised to characterise different policing actors. These theories point to current gaps in our understanding of online illegal drug and wildlife trades policing, the different actors who come together to conduct these disruptions, and the activities they each perform.

2.1 Online illegal trade

Society has brought people together to exchange goods and services in places we call markets, both offline and more recently online, which have enabled the sale of both legal and illegal products. When one thinks of online illegal trade, it is easy to picture a secret purely criminal marketplace trading in firearms, stolen personal and financial information, malware, and/or child sexual exploitation materials. However, online illegal trade has recently also been conducted on legal platforms for all to see. The different layers of the web are detailed before the types of platforms these trades are conducted on are described further.

2.1.1 The Surface, Deep, and Dark webs

Before detailing the types of platforms housing illegal trades, it is important to describe different parts of the web and where these platforms lie. The most common way of describing layers of the web is with the picture of an iceberg (see Figure 2.1). The surface web, or World Wide Web, consists of websites indexed by search engines which users can search for and visit without barriers. However, this is only a very limited openly visible part of the web, while others, called the Deep and Dark webs, are more opaque. The Deep web consists of password-protected web forums, chat services, and file sharing, which are not accessible through traditional search engines and much more numerous than surface sites (Bergman, 2001). The Dark web is a part of the Deep web that is only visible to users who have installed specialised software to access them, such as The onion router (Tor) and I2P (Bartlett, 2014), tools that encrypt communications and maintain anonymity for users by routing connections through a "series of tunnels" to distort the original IP address (Dolliver et al., 2018). The Dark web therefore offers a highly anonymised environment, which can be used for malicious purposes.

It has been noted that the Dark Web and the anonymity and privacy it offers are not necessarily the problem, and that not everything on the Dark Web is bad. The problem on these platforms (and offline) is criminality itself, which can thrive given these capabilities. Indeed, while not all Deep and Dark web users have malicious intents, many use these corners of the web to plan and execute illegal activities such as hacking, information theft, and terrorism (Bartlett, 2014; Weimann, 2016). One of these illegal activities has been the trade of illegal products and services, which is taking place both on the Dark web, including on Darknet markets, and on the surface web.

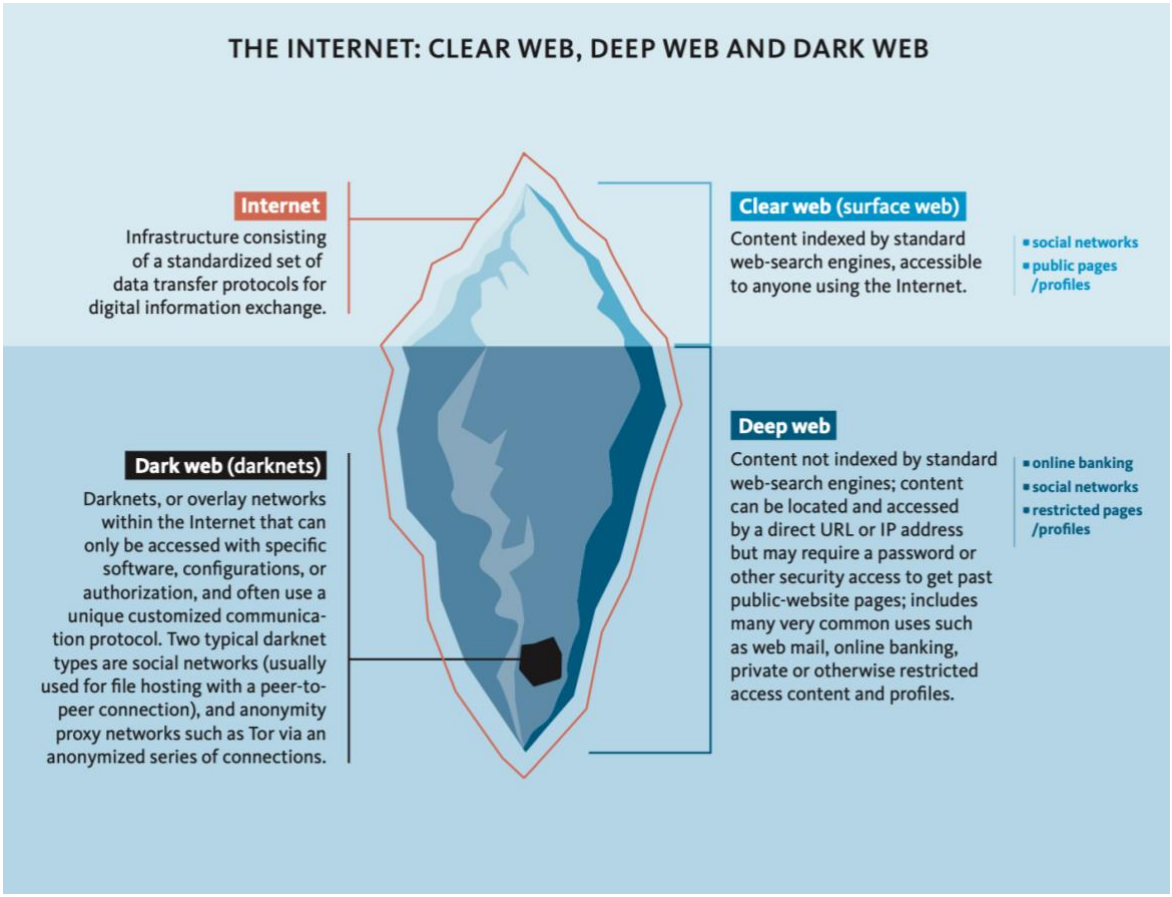


Figure 2.1: The Internet: Clear Web, Deep Web and Dark Web (UNODC, 2021c)

Darknet markets enable the sale of illegal goods and services online (Décary-Hétu and Giommoni, 2016), including but not limited to narcotics, firearms, stolen personal and financial information, and cybercriminal services such as malware for sale (Kigerl, 2018). This project includes cryptomarkets, online marketplaces only accessible through Tor within its definition of Darknet markets. Barratt et al. (2016) describe Darknet market users as relatively

young (22 years old on average), mostly male (82.3%), and white (91.5%). The majority of users are employed (55%) but a significant share are still students (35%). A relatively high proportion are educated, with 82.4% having completed secondary school and 38% holding a university degree. Additionally, because of their lucrative nature, Darknet markets have become professional business activities rather than hobbies for most users (Kigerl, 2018; Lusthaus, 2018). This therefore impacts the behaviours and motivations of administrators (the people running the marketplaces), vendors, and buyers.

Several academic studies have investigated specific Darknet marketplaces such as the earliest cryptomarket Silk Road (Barratt et al., 2013; Christin, 2013; Van Hout and Bingham, 2013; Aldridge and Decary-Hetu, 2014; Phelps and Watt, 2014), the largest and most prolific Darknet market to date AlphaBay (Paquet-Clouston et al., 2018), and one of the largest recent Darknet markets DreamMarket (Zhou et al., 2020). These projects aimed to better understand these markets' functioning, the products they sold, prices they offered, quality ratings they generated, and more. These articles report that these Darknet markets were modelled on legal online platforms; they show pictures of the products for sale, indications of where the products originate from, where they can be shipped to, and allow buyers to contact vendors (Bartlett, 2014; Mireault et al., 2016). These marketplaces cater mostly to drugs (Christin, 2013), the transactions they house generate excellent feedback (*Ibid*.), and their vendors are likely to use several aliases on one marketplace or trade on several Darknet markets (Soska and Christin, 2015). Although vendors and buyers can be located anywhere in the world (Broseus et al., 2017) drug offerings have been found to originate from a small number of consumer countries rather than production countries (Dittus et al., 2018; Norbutas, 2018). Overall, large profits are to be made on Darknet markets, which have encouraged these marketplaces to attack one another to win market share (Zhou et al., 2020). These competitions have taken the form of Denial of Service attacks for instance, to prevent competing marketplaces from remaining online and providing their services to users.

However, these financially-motivated attacks are not solely happening between cybercriminal marketplaces, they are common between individual cybercriminal traders too. Indeed, understanding buyers' specific needs, administrators have been taking advantage of them by shutting their sites down suddenly and taking the money held in escrow until

purchases were confirmed (Europol, 2017b). Vendors have also been defaulting on their orders or making opportunistic exits if suffering from bad ratings (Cabral, 2012), therefore causing conflicts between participants (Morselli et al., 2017; Bradley and Stringhini, 2019). These internal conflicts have provided the Police as well as moral crusaders (Becker, 1963) - members of society who disagree with certain practices on moral grounds and work to disrupt them (initially coined for people morally objecting to drug use) - with additional techniques to disrupt these Darknet markets based on real behaviours they have witnessed on these marketplaces. These complement their initial strategies and don't appear as enforcement-led interventions.

As well as marketplaces dedicated entirely to illegal trade, legal platforms on the surface web have also been used for illegitimate purposes. Numerous news and academic articles have pointed to increasing amounts of these trades on legal websites and social media applications, more broadly accessible and convenient than Darknet markets (Babb, 2014; Thanki and Frederick, 2016; EMCDDA and Europol, 2019; Moyle et al., 2019). As such, these trades were witnessed on auction and trading websites such as eBay (IFAW, 2004, 2008b), Craigslist (IFAW, 2014c), and Preloved (IFAW, 2018a), social media applications including Facebook (WJC, 2018a) and Instagram (Babb, 2014; Moyle et al., 2019), and instant messaging applications such as WeChat (WJC, 2017a) and WhatsApp (WJC, 2018a; Moyle et al., 2019). Indeed, these legal platforms offer the ease and convenience that Darknet markets provide while also allowing more users to get involved, as these sites are more widely available and more easily accessible for less skilled users. Anonymity might not be achieved to the same degree as on Darknet markets, because users' profiles either use their real names or are linked to their phone numbers or email addresses when they use pseudonyms. However, the use of private 'Groups', which the wider public cannot see or enter, as well as that of private messaging, which is often encrypted, render trades more difficult to monitor (EMCDDA and Europol, 2019). The encryption of social media and instant messaging applications is now also being used for illegal trading purposes. This has allowed certain illegal trades to thrive on these sites while remaining largely undetected, as the sheer number of users and listings are difficult to monitor, and these types of trades have not been widely researched (*Ibid*.).

2.1.2 Drug and wildlife products

Many products and services are bought and sold on the Dark and surface webs. However, this thesis focusses on drugs and wildlife to paint a better picture of online illegal trade policing in these two cases. This section starts by defining what drug and wildlife products are, describing their provenance, the groups involved in their trade, and the motivations of their buyers, before showing the similarities and differences between these two trades, warranting their simultaneous analysis.

Drugs are chemical agents available in different forms and from various sources that alter biochemical and physiological processes (UNODC, 2021b). Some of these chemical agents are naturally occurring (UNODC, 2013), found in plants such as cannabis flowers, coca leaves (EMCDDA and Europol, 2013b), and certain poppy seeds (EMCDDA and Europol, 2016b). Other chemicals are semi-synthetic, involving natural materials that were chemically manipulated (UNODC, 2013), such as opiates including heroin obtained by the acetylation of morphine, itself coming from opium (EMCDDA and Europol, 2013b). And finally the rest are fully synthetic, created entirely by laboratory manipulation, including amphetamines first synthesised in Germany in 1887 to stimulate the central nervous system (UNODC, 2013), and ecstasy originally used to stop bleeding and then as an aid for communication and emotional expression by psychotherapists (EMCDDA and Europol, 2013b). Although drugs are tackled as a broad concept as part of this thesis, they encompass very different products described in the rest of this section, from legal to illegal substances, used for stimulation, recreation, or medication (UNODC, 2013), and they are therefore traded in slightly different ways. These differences are acknowledged in this chapter before these various drugs are referred to using the same terminology in the subsequent empirical chapters.

It is difficult to estimate how many people purchase medicines online (Sugiura, 2018), but Europe, with an estimated drug market valued at €2bn per month (Kruithof et al., 2016), is recognised as a hub for the production of synthetic drugs. The Police are trying to address this hub, but the European continent has no control over the sourcing of natural drugs coming from other regions of the world (Europol, 2006). The commodity chains in all three forms of these drugs, the sequence of operations from initial extraction or production to final consumption, are fragmented into hubs dealing with sourcing, production, smuggling,

transport, distribution, and sale (Malm and Bichler, 2011). Overall, traffickers sell drugs to make money, because there are few barriers to entry and few specialised skills are needed in the chain (Sandberg, 2012). Organised Crime Groups are groups of three or more individuals whose purpose is to perform criminal activities ("Serious Crime Act," 2015) in view of obtaining financial or other benefits, following an internal structure, and having existed for some time before and after the commission of an offence ("United Nations Convention against Transnational Organized Crime," 2000). These groups are involved in several of these hubs and are increasingly trafficking several drugs at a time to respond to poly-drug consumer profiles and increased profits (Europol, 2004, 2005, 2011a). These trades therefore threaten human, military, political, and economic security (Swanstrom, 2007), as the income generated then allows these Groups to fund terrorist activities and more dangerous crimes (EMCDDA and Europol, 2019), not only in their countries of operation but also in Europe, as they have ties with European countries (Europol, 2008).

Due to the cost of prescription medication in the United States, the availability of medication on the Internet (Sugiura et al., 2012), and the lack of capacity to significantly control the Internet (Lavorgna, 2016; Sugiura, 2018), the country is suffering from a large number of cheap counterfeits provided on illegal online pharmacies. These cybermarkets illegally distribute prescription drugs that can be ineffective, out of date, contaminated, unapproved by regulatory authorities, dispensed without valid prescriptions, marketed with fraudulent health claims, or intended for criminal use (Maxwell and Webb, 2008; Sugiura et al., 2012; Mackey and Liang, 2013; Krebs, 2015; Scammell and Bo, 2016). This surge in illegal medication offerings has been driven by high demand and therefore profit incentives (Sugiura, 2018). Indeed, Krebs (2015) noted that American customers are more likely to purchase necessary medication over the Internet contrary to their Western European and Canadian counterparts who are only looking to supplement their lifestyles. When customers are not directly looking for medicines online, they can also receive spam emails about purchasing cheap medicines in a confidential and convenient manner, fuelling demand even further (Krebs, 2015). In both cases, the illegality of these products makes them fit for our analysis.

Another recent threat in drug trafficking has been the emergence of New Psychoactive Substances, a broad range of new chemicals intended to mimic the effects of existing

controlled drugs, but themselves not yet controlled under international drug laws (EMCDDA and Europol, 2013b). These are often called 'legal highs' as they have not yet been deemed illegal (EMCDDA and Europol, 2012b) and they pose issues of identification, even for specialist laboratories (EMCDDA and Europol, 2008). The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), which provides the European Union and its Member States with a factual, objective, reliable, and comparable overview of European drug problems (EMCDDA, 2021), has been conducting yearly drug snapshots alongside Europol since 2005. Both agencies have been monitoring the number of New Psychoactive Substances identified on the continent, the amount of sellers supplying them online and offline, and the harm they have caused. Annual New Psychoactive Substances numbers have grown from 14 identified substances in 2005 (EMCDDA and Europol, 2005) to 101 at the peak in 2014 (EMCDDA and Europol, 2014a), then going down slightly in subsequent years. 47 deaths linked to New Psychoactive Substances were reported on the continent between 2013 and 2014 (Europol, 2014b). Prices for these and other drug products have been noted to be abnormally high and unexplained by the low costs of production (Sandberg, 2012), instead stemming from demand from buyers. Indeed, strain theories explain that people who experience high periods of stress and deprivation due to social and economic conditions, among other things, are more likely to break rules they might usually comply with (McLaughlin and Newburn, 2010; Maguire et al., 2012), in this case the consumption of illegal substances. The products and services on these sites have therefore become a need in buyers' precarious situations, sometimes explaining their willingness to pay a premium for them. Such premiums are also witnessed in online illegal wildlife trade.

Wildlife consists of any wild plant or animal, whether indigenous or exotic, and any derivative thereof (Bürgener et al., 2001). This term is often used in conjunction with that of 'trafficking', the process of illegally trading such wildlife, whether alive, dead, or in derivative products, including collection, harvesting, possession, processing, acquiring, transporting, importing, exporting, selling, bartering, or exchanging (Bürgener et al., 2001; Lavorgna, 2014b). This process is diverse and complex and involves a variety of perpetrators rather than just one mastermind (Moreto and Clarke, 2013). Just like other illegal trades, estimates have been drawn about the potential value of wildlife, based on declared values at customs and accounting for large variations in the black market, ranging from $10bn to $20bn per year

(South and Wyatt, 2011). Wildlife can be traded in different forms, including live plants and animals and plant and animal products. Some live species are legal to trade, but others are restricted by the 1975 Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), an international agreement ensuring wild animal and plant trades do not threaten their survival. The convention has been regularly updated and now counts 183 signatories and more than 35,000 protected species, including 30,000 taxa of plants and 5,000 taxa of animals (CITES, 2020b). CITES identified three levels of restrictions, including plant and animal species threatened with extinction whose trade is banned except in exceptional circumstances; vulnerable species whose trade is restricted to avoid utilisation that would be incompatible with their survival; and species that are protected in at least one country and whose trade control requires assistance (CITES, 2020a).

Wildlife products also exist in two different forms, those directly stemming from plants and animals, such as timber, rhino horns, and pangolin scales, and those further manufactured, including ivory ornaments. Wildlife is therefore a concept as broad as that of drugs, and although different wildlife species and products are detailed in this section, the rest of the thesis refers to them as one category to simplify its analysis. However, live animals and animal products have received more attention than plants in recent academic literature and other publications (Margulies et al., 2019; Lavorgna et al., 2020). Live specimens and products involved in these trades vary throughout the years and across locations. Organisations like IFAW provide thorough reviews of trades in various countries at regular intervals. In their most recent publication on this matter, they reported that 80% of trades were in live specimens, with reptiles being the most traded followed by birds, and that animal products constituted the other 20%, mostly related to ivory (IFAW, 2018a). Countries involved in this trade also varied throughout the years and depending on the species and products for sale. However, Europe has been identified as an important market in both source and destination for birds, mammals, reptiles, fish, herbs with medicinal properties, and timber (Europol, 2013b).

Buyers are motivated by these wildlife purchases for several main reasons: the rarity of certain products and species which they hope to acquire before they are extinct (Courchamp et al., 2006; Europol, 2013a; Holden and McDonald-Madden, 2017); the trusted medicinal

benefits of certain plant and animal products (WJC, 2016c, 2020c); and their use as food, pets, ornaments, and even fashion (UNODC, 2021a). These motivations justify the price premiums applied to the products and the sizeable profits available to financially-motivated vendors who perceive very low risks from getting involved in such trades (Europol, 2013a; Lavorgna, 2013). Several of these vendors, or traffickers through the previously described chain, take the form of Organised Crime Groups often using violence and corruption to reach their goals, and these networks have transformed the critical conservation issue of wildlife trafficking into a financial crime threatening global security (IFAW, 2013; Europol, 2015a; Viollaz et al., 2018). However, evidence suggests most of these crimes are committed by opportunistic individuals, such as local farmers supplementing their income (Lavorgna, 2013). Most jurisdictions have some form of animal protection law (Nurse, 2013) and the Police have been addressing this type of criminality, most recently through internationally coordinated seizure and arrest operations (WCO, 2016a, 2019; Europol, 2020a, 2020g). However, and although criminal traders are conscious of such targeting, these enforcement activities are still seen as too sporadic to raise the perceived risk of this activity (Lavorgna, 2014b). Indeed, these trades have kept growing in recent years and have taken to the Internet for more connection and accessibility.

Drug and wildlife species and products are similar in many respects. Indeed, they both exist in similar forms from natural to manufactured. They are two of the four most traded and profitable illegal products sold online (EMCDDA and Europol, 2017a, 2019), and involve similar financial and opportunistic motivations from their traders (South and Wyatt, 2011), including Organised Crime Groups. Many of these groups traded drugs in the 1970s and 1980s, as this trade wasn't seen as very risky. They recently moved to trading wildlife products for similar reasons, following the extensive war on drugs and the commitment of Police resources which have not yet reached wildlife (South and Wyatt, 2011). Drugs and wildlife are physical products that need to be shipped following online orders, giving the Police and Customs the opportunity to intercept them. Despite production and poaching taking place in source countries far from demand countries, both products are likely to be traded nationally (Interpol and IFAW, 2013; Dittus et al., 2018), and stem from a deep need from buyers often willing to pay premiums for them. Drug and wildlife species and products have been compared in the literature for their similar trafficking stages and their use of similar smuggling

routes, often simultaneously (Europol, 2021e), as described in crime scripts detailing the steps and illegal actors involved in these trades (South and Wyatt, 2011; Lavorgna, 2014a, 2014b). As legal markets exist for both drugs and wildlife (Sugiura et al., 2012; Lavorgna, 2015b), these products are controlled through national, international, domestic, and transboundary legislation and regimented by legal classifications applied to different species and drugs (IFAW, 2005). Finally, they both have deep impacts on national economies and security (Viollaz et al., 2018), including health and violence in consumer countries, and corruption and destruction of the environment in source countries (South and Wyatt, 2011; Europol, 2012; IFAW, 2013).

However, there remain several differences between illegal drug and wildlife products. Drugs, whether sold online or offline, have been the most traded illegal product across continents for decades, with an estimated value of $20bn per year in Europe alone (UNODC, 2021b), and a volume of drug users which had risen at an accelerated rate during the COVID-19 pandemic (EMCDDA, 2020; UNODC, 2020c). Drugs have therefore been extended a priority policing status long before their sale began on the Internet, which is believed to have started in the early 1970s on online academic networks (The Economist, 2014). Drugs are the products that have received the most attention related to their Internet-mediated trafficking (Lavorgna, 2014a). However, wildlife species and products are just now starting to be referred to as a mild threat (Europol, 2017g) following years of lobbying from welfare organisations, but they have not yet been offered the same extensive Police commitment (South and Wyatt, 2011). Additionally, much research has been undertaken on drug trade, its volume, value, and characteristics, which cannot yet be said for wildlife (South and Wyatt, 2011), as only broad estimated ranges are available, such as illegal wildlife trade being valued between $7 and $23bn per year (United Nations Environmental Programme and Interpol, 2016). Many non-profit organisations have been concerned with animal welfare, including their illegal trade, and they have worked together to reduce these trades' impact on species and the environment as part of organisations such as the Coalition to End Illegal Wildlife Trafficking Online. Fewer and more targeted organisations focus on drug trade, often focussing on prescription drugs such as the Centre for Safe Internet Pharmacies. Although both types of trades are currently happening on surface websites and social media applications which have a large global reach (Lavorgna, 2015a, 2015b), drugs are still largely available on the Darknet.

This priority enforcement status therefore shows the power the Police conjure, driving drug sales to the Darknet for anonymity and security purposes through fear of identification and arrest, and making them the main use case for such Darknet services, which has not been the case for wildlife (Lavorgna, 2014b; Harrison et al., 2016; Lavorgna et al., 2020).

Drugs and wildlife being similar in many foundational respects and yet so different, we have much to gain from researching both of these products' policing as part of the same study and not treating them as completely disparate phenomena. This thesis therefore gathers complementary insights and highlights the main differences in their policing, which will provide useful strategies for their future individual policing on both the Dark and surface webs. Although it might initially appear that this strategy would only allow for a better understanding of online illegal wildlife trade policing following the more thoroughly studied illegal drug trade (South and Wyatt, 2011), it has been argued that the war against drugs has gone on for decades and that the situation is currently at its worst (Collins and et al, 2020). Disruption methods used in illegal wildlife trade could therefore be investigated and offer insights about the policing of the evolving drug trade.

2.2 Policing online illegal trade

Following an examination of online illegal trade, the platforms it takes place on, the users it attracts, and the products it involves, this section now turns to the ways online illegal trades, among other cybercrimes - offenses that involve the use of new communication technologies for their commission (Leukfeldt and Yar, 2016) - have been policed.

2.2.1 The Police

The word 'Police' takes several forms from a common noun referring to the civil force of a State, the organisation engaged in enforcement, and the members making up the Police force, to a verb suggesting the maintenance of law and order and the enforcement of regulations (Brodeur, 2010). The Police as an institution was born in France in the 17th century under the reign of Louis XIV in order to regulate aspects of public life. Its appearance in the UK ensued in 1829, although only in the metropolis and the process of extension to the rest of the country was then gradual (Button, 2019), putting the emphasis on the prevention and detection of crime. The Police apparatus, a group of professionals employed by the State, has a broad mandate for enforcing laws, maintaining order, and ensuring public safety (Crawford, 2003). Over the last decades, academics and researchers have aimed to classify the various components of the Police organisation, noting the different agencies, specialisations, and challenges it involves, specifically on the Internet (Wall and Williams, 2007).

Leading British academics in the policing field have designed policing frameworks to bring together these various components. For instance, Johnston (1992) distinguishes between public, private, and 'hybrid' policing sectors. For him, 'hybrid' policing includes bodies engaged in functions related to State security (e.g. immigration staff, prison officers, Ministry of Defence Police…); special Police forces (e.g. British Transport Police, parks and docks Police forces…); departments of State and municipal bodies engaged in regulatory, investigative, and enforcement functions (e.g. Board of the Inland Revenue Investigation Unit and HM Customs, Environment Health Officers, Trading Standards Officers, social workers…); and miscellaneous regulatory and investigative bodies, such as Post Office or BBC investigators. Although he argued these three sectors were increasingly connected, and the actions of one were likely to affect the others, they were not yet coordinated (Johnston, 1992). Jones and Newburn

(1998)'s four-fold classification includes Home Department Police forces, such as the Metropolitan Police Service; Other Bodies of Constables/Special Police Forces, such as the British Transport Police; Other public policing bodies, such as Environment Health Officers and Benefit Fraud Investigators; and Private security operations, such as staffed services, investigatory services, and installation of security equipment (Jones and Newburn, 1998). However, these and many other policing frameworks have not been updated to account for the technological evolution of crime and policing.

Indeed, the Police have been tasked with disrupting trade on Darknet markets, among other cybercrimes, as cybercrime rates have increased in recent years (Dupont, 2016a; Europol, 2017g) and are expected to keep rising in the future (Europol, 2017g). Goodman (1997) expressed concerns that "the Police [didn't] care about cybercrime", not only as a result of lack of training and technological understanding but also because emphasis was being put on violent terrestrial crime instead of smaller-impact cybercrimes, following the principle of *de minimis,* or minimal things, – "*de minimis non curat lex*" ("the law does not concern itself with trifles") (Wall, 2007a). But things have since dramatically changed (Broadhurst, 2006). Several organisations, not only in the UK, but also regionally and globally, have been founded in order to work towards understanding and disrupting these crimes. Their goal, just like for any offline criminal network, has been to target the largest Darknet markets in terms of vendors, sales, and products on offer (Europol, 2017b), infiltrate them to gather information (Poulsen, 2011), arrest their administrators, and take down their infrastructure.

2.2.2 Arrests and takedowns

Police responses to Darknet markets and online illegal trading websites so far have largely been focussed on traditional tactics, some arrests and several takedown operations having been performed by agencies around the world. Although many traders are never arrested, there have been several arrests of Darknet market administrators (United States of America Department of Justice, 2014a, 2016b, 2018a) and vendors (United States of America Department of Justice, 2015, 2016c, 2016a, 2018b). Sometimes such arrests require some luck and particularly other cybercriminal traders trading their accomplices' names for reduced sentences, as was the case for CardersMarket administrator Max Butler (Poulsen, 2011; Dupont, 2016c). This shows the diffuse nature of these markets and the difficulty in

establishing with any degree of certainty the precise location of an online offence (Paquet-Clouston et al., 2018) and the precise identity of an offender. These efforts by the Police have been argued to be too expensive and too slow (Decary-Hetu and Laferriere, 2015), and some therefore argue that they require potential sub-contracting to private industry (Hutchings et al., 2016), and consequently a shift in enforcement powers.

In addition, several major marketplace takedowns were performed in recent years, including four takedowns during the first half of 2019 – xDedic (Europol, 2019h), Wall Street Market and Silkkitie as part of Operation East River (Europol, 2019b), and Deepdotweb (Europol, 2019a) – and the takedown of DarkMarket at the start of 2021 (Europol, 2021c). Although such takedowns are intended to reduce the benefits of cybercriminal trading and increase its cost, effort, and perceived likelihood of detection (Hutchings et al., 2016), these have not been the observed effects over the long-run. Indeed, this method has been criticised in the literature - not only is it deemed not to be efficient and impactful enough (Poulsen, 2011), it is believed that such takedowns might actually strengthen activities on these marketplaces (Duijn et al., 2014; Van Buskirk et al., 2014). As such, these takedowns have been shown to increase trade and vendor revenues (Ladegaard, 2018), to incentivise technological innovation (Buxton and Bingham, 2015) through the use of more secure communication techniques, encryption, two-factor authentication, and architecture decentralisation, and to foster competition (Décary-Hétu and Giommoni, 2016).

Indeed, Ladegaard (2019) found that the shutdown of Silk Road (and numerous other Darknet marketplaces after it) did not act as enough of a deterrent but instead spurred community and solidarity among its members. His analysis of three discussion forums shows that the Silk Road community came together as a collective unit to survive and migrate to a new platform following the crackdown. His finding was echoed by Cho and Wright (2019)'s analysis of Reddit and Dread data following the ban of forums related to Darknet markets on Reddit, which spurred a similar solidarity among the remaining members of the community. The shutdown of the Silk Road, among other illegal marketplaces, also led to the creation of other marketplaces for online illegal trade and the increase of such trade (Yip et al., 2013b; Van Buskirk et al., 2014; Décary-Hétu and Giommoni, 2016; Hutchings et al., 2016; Paquet-

Clouston et al., 2017; Ladegaard, 2018), therefore only displacing crime spatially (Reppetto, 1976).

Although Operation Onymous, a large-scale Police operation in November 2014 that targeted 410 cryptomarkets, including Silk Road 2.0, Cloud 9, and Hydra, decreased the total number of dealers registering on other marketplaces such as Agora and Evolution in the short-term, this effect was offset after only a couple of months (Décary-Hétu and Giommoni, 2016; Van Buskirk et al., 2017). Indeed, the number of active dealers recovered to its almost pre-operation level within a month and the number of sales was twice as high two months after the operation than it had been before (*Ibid*.). The deterrent effect of this operation, therefore, only lasted for two months before the size of the ecosystem recovered to its pre-operation levels (Van Buskirk et al., 2014; Décary-Hétu and Giommoni, 2016; Bradley and Stringhini, 2019), illegal trade was therefore not eradicated but again only displaced, this time temporally (Reppetto, 1976). Just as more general drug markets, these examples therefore show the resilience of Darknet markets and the ability of market participants to preserve levels of exchange despite external disruption pressures (Bouchard, 2007).

While this displacement narrative paints a somewhat futile picture of these operations, one should not be solely critical of these tactics. It should indeed be noted that these operations likely incurred costs on these Darknet markets, which had to invest time and resources into protecting themselves more effectively. This might have weakened them at least partly. Additionally, the way in which the Police perform these takedowns can also have a heightened impact. Operation Bayonet in July 2017 consisted of the Federal Bureau of Investigations closing Alphabay but not taking responsibility for its closure, as it had done for other marketplaces in the past. This led users to believe they had been victims of the administrators' exit scam, closing down the site and leaving with the money held in escrow until transactions were confirmed. Bradley and Stringhini (2019) showed that this operation generated many forum conversations between users, as well as leading some of them to reconsider using these marketplaces altogether. Indeed, this closure led to the creation of a number of smaller vendor shops, but these new marketplaces did not collectively meet the former scale of Alphabay, suggesting an overall decrease in illegal Dark web activity (Europol, 2017b, 2019g).

Bhaskar et al. (2019) also argue that users might be more affected by shutdowns should they believe that their identities have been compromised and found by the Police. This was the case when Hansa was run as a honeypot in 2017 as the Police took over the market and gathered participants' personal details while it was seemingly running normally. This is therefore another area to explore with regards to these takedowns. Although this method has been heavily criticised, the Police are making strides to perfect the way in which they conduct these operations in order to have the highest impact on Darknet market users. In fact, Europol have deemed arrest operations Onymous in 2014, Alphabay/Hansa in 2017, and East River in 2019 as three of their 20 most noteworthy overall operations (Europol, 2019c). For 18 months, the Federal Bureau of Investigation alongside the Australian Federal Police also ran its own encrypted messaging platform, ANOM, to gather details about criminal activities, including the international trade of illegal drugs, leading to more than 800 arrests in June 2021 (Europol, 2021a). The consequences of this novel and sophisticated operation on cybercriminal traders are still to be seen. Other policing tactics not targeting infrastructure but instead the connections between people have also been explored, following behaviours exhibited by cybercriminal traders themselves on these marketplaces. Indeed, the Police have not been disrupting these trades on their own, but they have relied on other groups and individuals to do so.

As a contrast to the Police, the word 'policing' relates to a broader sense of order and security, including activities such as maintaining order, preventing, surveying, and investigating deviant acts, involving both the public and private spheres (Brodeur, 2010). It is argued a vast bulk of policing is carried out by people and organisations other than the Police (Rawlings, 1995), which is particularly the case for the policing of the Internet (Wall, 2007b).

2.3 Policing online illegal trade with others

The above operations – arrests and takedowns - have been mostly conducted by the Police, though not without external support. Indeed, the State Police only became the dominant model in the delivery of policing with the emergence of the industrial economy at the end of the 19th century, its responsibility becoming firmly located within the State (Crawford, 2011). The State Police therefore eclipsed other private policing arrangements which had been in place until then, as individuals and organisations defended themselves by employing their own protection mechanisms (Johnston, 1992). These external arrangements are still active in large numbers (Crawford, 2011; Wakefield and Button, 2014) participating in the maintenance of peace and order, investigation of crime, and brokering of information (Jones and Newburn, 1998) today (Jones et al., 2017). Several examples are available of Police agencies receiving support from and cooperating with other agencies and external entities in the way of a network in the past.

In this policing context, a network takes the form of various groups collaborating and coordinating interventions, which is deemed vital for the policing of illegal trade (International Compliance Association, 2020) and organised crime more broadly "because it takes a network to defeat a network" (IFAW, 2018a). Pink and White (2016) add that "for collaboration to be meaningful, there has to be a development of trust and common purpose, as well as sharing of information and resources". Such trust between parties involves making "correct expectations about the actions of other people" (Dasgupta, 1990), namely performing their part of policing operations. This collaboration became a requirement as the Police had to deal with ever-increasing and varied amounts of crime. However, trust could not be given to just anyone, so it seems appropriate that the Police started to collaborate with other Police forces they might better understand and be able to form correct expectations about.

2.3.1 Support from other Police agencies

At the turn of the century as the world became increasingly globalised with better communication and transportation networks, crime too began to cross borders more easily and frequently. In response to this more negative side of globalisation, Police forces started

to cede some of their sovereignty and to diminish their monopoly on the legitimate use of force by engaging in international Police operations against terrorism and drug trade with other forces around the globe (Friedrichs, 2008). Despite organisations such as Interpol and Europol having already been created in the 20th century, the Police further focussed on developing specific measures and transnational capabilities to make these fights global. Indeed, the United Nations Transnational Organised Crime Convention was established in 2003 as the main international instrument in the fight against organised crime, including an Article specifically centred around Police cooperation. The Council of Europe's Innovative Cybercrime Convention was then established in 2004 as the only binding international instrument on the issue of cybercrime for international cooperation between signatories, among others (Broadhurst, 2006). These regional groups and collaborative efforts are still alive today in many criminal realms, with no less than 51 Police cybercrime cooperative initiatives having been identified and analysed in 2016 (Dupont, 2016b). Global enforcement organisations go from strengths to strengths and continue to oversee major international operations by coordinating several national forces. Many of these interventions are cyber-related as various examples of market takedowns and mass arrests show, given such offenses were similarly prioritised in the involved jurisdictions (Wall, 2007b). However, where Police skills and resources weren't enough, the Police also secured support from external entities, Private Policing.

2.3.2 Support from Private Policing

Before explaining how the Private Police has supported the Police in their disruption operations, it is important to define what is meant by this concept and how it has evolved since its earliest form in the 18th century, when a small number of private citizens volunteered to undertake State protection roles due to a lack of public enforcement (Critchley, 1978). The Private Police has been defined as the free market provision of security services, contrasted with its State provision by the Police (Jones and Newburn, 1998).

The Private Security Industry is the field of Private Policing that has received the most attention (Brodeur, 2010). Private Security Industry agents are mostly associated with order maintenance, loss reduction, and protection for a fee, although these functions are not common or exclusive to all of the activities of the industry (George and Button, 2000). The

industry is recognised as taking three main forms: staffed services (such as security guards in shopping, business, hospital, or university precincts), security equipment (including CCTV, home alarms, and retail security tags), and investigation (Jones and Newburn, 1998), which are performed by individuals and groups working for the private sector rather than the State. In light of these various services, a large growth in Private Security Industry provision has been noted (Johnston, 1992; Jones and Newburn, 1998), as the State has been unable to meet demand for services and the private sector has therefore filled that gap (Button, 2019). In fact, the Private Security Industry likely outnumbers the State Police in terms of employees, though the roles they perform are deemed insignificant and largely overlapping with that of the Police (Herbert, 1999). While this claim might hold true for some forms of policing, it will be refuted in the case of online illegal trade policing. Beyond its commercial aspects, Private Policing also takes the form of in-house security and voluntary policing activities (Button, 2019), which are discussed in more detail in the Classification of policing section of this chapter.

The Police have received support from the Private Police before and during the cyber era.

In the early 2000s, Dupont (2004) argued that security should be conceptualised as produced by a network of actors of which the State Police only constitutes one node, even offline. Later, he then expanded on this notion by providing a summary of four key stages and models of cooperative policing, from privatisation, to bureaucratisation, hegemonism, and polycentrism today (Dupont, 2016b). As such, in the late 1800s, the industrial revolution and expansion of international commerce and investments required the protection of firms' financial and commercial interests. This led to the privatisation of these security initiatives, given the lack of information exchange between private companies and State Police. In the early 1900s, administrative structures were put in place to facilitate global communication and information exchange while respecting national sovereignties, giving birth to organisations such as Interpol. Such bureaucratisation, however, led to the emergence of several procedural constraints security professionals across the world had to follow. Despite numerous bilateral partnerships, this gave the impression that hegemony rather than cooperation became the ultimate goal and it encouraged individual actors to break away from the system and come up with their own ad hoc processes for Police cooperation. Today,

Dupont (2016b) argues the system is polycentric, bringing together the previous three models, overall reflecting a new global policing architecture where several entities have their role to play due to their specialised skills or preferential position in the system (Cherney et al., 2006). Indeed, any organisation from an Inter-Governmental Organisation (IGO) to a Non-Government Organisation (NGO) or a private company can and has taken the reins of a cooperative initiative, often with greater efficacy than the Police (Dupont, 2016b). Enforcement gaps have therefore been filled by IGOs and NGOs taking on duties such as raising public awareness, enforcing legislation and carrying investigations if it is not abided by, and influencing legislative and political agendas (Nurse, 2013). The impact of these NGOs is believed to be vital in the effective enforcement of wildlife legislation specifically, which cannot be fully fulfilled by public agencies (*Ibid*.). Private organisations have also been fighting terrorism (Petersen, 2008), establishing anti-money laundering regulations (Oliveira, 2014), and controlling crime on the waterfront through stakeholders as diverse as shipping companies, labour on the ground, and legal authorities (Brewer, 2014). Indeed, "policing is not simply the preserve of the Police" (Flanagan, 2008) and partnerships are now in place to respond to crime, investigate crime, share intelligence, share knowledge, and work with others (Wakefield, 2003). However, it was noted an entrenched lack of trust between public and private actors has come in the way of these partnerships, as it is a prerequisite for the success of these collaborative operations (Bures, 2013). These partnerships and issues persist in the era of cyber threats.

Although terrorism, drugs, and maritime security, among others, are still ongoing fights, and in certain cases have been aggravated by technology and connectivity, private support has also played a big part in the Police's fight against cybercrime. It was noted early on that the Police only played a small part in governing the Internet and therefore needed to forge relationships with other nodes within the network of Internet security, as well as acquiring new knowledge and capacity where needed (Wall, 2007b). When it comes to the Internet, the Police no longer have a monopoly in the delivery of security (Dupont, 2016a). Indeed, some have argued that Internet Service Providers, organisations that provide services for accessing and using the Internet, and Internet users themselves must be primarily responsible for cleaning up cyberspace, as they hold responsibility for its infrastructure and content (Jewkes and Yar, 2011). Additionally, as will be detailed further in a later chapter, the

"platformitisation" of the Internet, its division in discrete sites, has meant that individual administrators have the power to govern their own platforms (Helmond, 2015). There are several examples where the Police are not necessarily the best placed or most knowledgeable to disrupt these cybercrimes, at least not on their own, as they are seen as ill-equipped (Wall, 2007b) and require support from partners. Indeed, policing cybercrime requires collaborative responses from various agencies, whether in the public or private sectors, and collaboration between these entities should be prominent in this policing (Attrill-Smith et al., 2019). Already in the late 1990s, Wall (1998) identified several groups of actors involved in policing the Internet to various degrees, including Internet users in the virtual communities they were part of; State funded non-public Police organisations including governmental authorities controlling Internet traffic; and State funded public Police organisations. Despite security not being the main role of private non-security industry companies, which instead focus on making profit (Bures, 2017), they are often better-placed and better-resourced to understand and minimise risks due to their knowledge and skills, which the State might not possess (Carrapico and Farrand, 2017). Private organisations have therefore partnered with public ones and the Police for various cyber-related issues, such as managing telecommunications and other critical infrastructure protection (Shore et al., 2011), providing reliable Internet and Information Communication Technology access, as well as relevant information about threats and vulnerabilities when available (Bossong and Wagner, 2017), providing information for data system break-ins (Leppänen and Kankaanranta, 2020), and many others. Beyond corporations, individuals can also take part in cyber-governance, as advocated in bottom-up decentralised approaches and technology activism where those most affected by policy measures get to participate when needed (Milan and Hintz, 2013). International cooperation is also needed between public and private practitioners and academics (Sarre et al., 2018), and a recent study showed an increase in international and interdisciplinary academic studies in the field of cyber security was underway (Payne and Hadzhidimova, 2020).

Some actors have also been involved in the policing of cybercrime without meaning to be.

2.3.3 Inspiration from cybercriminal traders

In a purely hypothetical world, the standard model of a market economy would take for granted consumers not overspending but instead staying within their budget, as well as vendors always delivering the goods and services they promised to buyers (Dasgupta, 1990). However, in reality and to a larger extent on the current online marketplaces, this is not always the case. Credible punishments aimed at incentivising participants to fulfil their end of agreements and contracts have therefore been put in place, in the form of reputation (Schelling, 1960; Dasgupta, 1990; Dixit, 2004). Dasgupta (1990) defines reputation as "a capital asset" central to all transactions that can be built up slowly by pursuing certain courses of action and destroyed, often quickly, by pursuing others. In the case of online trading, a good reputation can be attained by producing good quality products and services at a reasonable price. On the contrary, not delivering on one's promise to send a product acquired by another participant could lead to a poor reputation. Participants' decisions about whether or not to trust one another in a market is dependent on their reputation, hence economic agents' concerns to establish them for their future transactions (*Ibid*.). The way they have done so is through enhancing the reputational mechanisms used to provide positive or negative signals to future potential customers. It is important to note the centrality of these mechanisms to the good functioning of markets as a whole, even in vastly different contexts (Milgrom et al., 1990; Greif, 1991). For instance, looking back to the Champagne Fairs of Medieval France, private judges recorded information on past transactions so that traders could be appraised of who had a bad record and should therefore be avoided in future dealings (Milgrom et al., 1990). Similar reputation mechanisms have been employed for online trading.

Markets in which vendors cannot reliably signal trust and product quality may experience failure, as a greater number of vendors may have an incentive to offer products of lower quality which will not satisfy buyers. In light of this, and at a time when Darknet markets were but a distant utopia, Akerlof (1970) famously coined these "markets for lemons" and argued for the use of reputational tools to avoid such outcomes, including brand names, licensing, and guarantees. This concept has since been applied to cybercriminal markets specifically (Hoe et al., 2012) and has given rise to terms such as 'scammers' and 'rippers' to describe

vendors not living up to their end of transactions (Herley and Florencio, 2009). The addition of reputation mechanisms aimed at assessing participants' trustworthiness and avoiding such negative experiences have therefore lessened the risks associated with these interactions (Lusthaus, 2018), as participants learn to make "correct expectations about the actions of other people that have a bearing on [their] own choice of action when that action must be chosen before [they] can monitor the actions of those others" (Dasgupta, 1990). Overall, these mechanisms have therefore enhanced cooperation and built trust between market participants, so much so that illegal markets have tried to recreate these legal structures underground.

Underground economies have been associated with high levels of uncertainty, which online illegal trade on Darknet markets and elsewhere are equally affected by (Yip et al., 2013b). Indeed, in such economies, buyers are unable to ascertain the quality of the goods and services sold and to verify the identity of market participants. Meanwhile vendors have no credible way of disclosing quality, are not regulated, and have been known not to provide the goods and services that have been paid for (Herley and Florencio, 2009). This doesn't solely happen on Darknet markets but also on legal platforms, such as eBay. For instance, several scammers have been arrested for selling legal products on the auction website that they never owned and had no intention of sending to their buyers (Conradt, 2012; United States of America Department of Justice, 2014b). That principle could therefore be exacerbated on cybercriminal marketplaces or for illegal products because buyers are unable to report these scams to the Police, as they would reveal their own involvement in illegal activities (Holt et al., 2016).

A number of steps have been taken on Darknet markets in order to mitigate these risks. In particular, Darknet market administrators have put in place a system to reduce identity and quality uncertainty and to convince buyers to trade with anonymous vendors (Yip et al., 2013a). Upon their arrival on a Darknet market, vendors are encouraged to provide a sample of their product or service to marketplace administrators or other appointees, for them to verify their trustworthiness and the quality of their products and services. This initial vetting process then gives vendors the opportunity to display a "reviewed vendor" (Yip et al., 2013b), "trusted vendor" (Decary-Hetu and Laferriere, 2015), or "verified status" (Dupont et al., 2016)

badge for all buyers to see. Administrators have therefore found a way to encourage good quality and rendered issues of moral hazard less prominent than one might initially surmise (Bhaskar et al., 2019). The rating systems put in place both in legal and illegal markets have also been the subject of considerable research (Ba and Pavlou, 2002; Melnik and Alm, 2002; Resnick and Zeckhauser, 2002; Dellarocas, 2003; Cabral and Hortacsu, 2004; Houser and Wooders, 2006; Jin and Kato, 2006; Li, 2010; Cabral, 2012; Christin, 2013; Lafky, 2014; Rabby and Shahriar, 2016; Belleflamme and Peitz, 2018; Bhaskar et al., 2019). Based on past transactions, these reputational systems help vendors build credibility on these marketplaces and instil trust in buyers. Bolton et al. (2004) refer to these reputation mechanisms as 'indirect reciprocity' as trust on online markets relies on a trader having been trustworthy with others before, compared to traditional markets which rely on 'direct reciprocity' where traders have been trustworthy with the same buyer before. It was shown that 95% of given ratings on these marketplaces are 5 stars (Bartlett, 2014; Bhaskar et al., 2019), likely given by new buyers (Dupont et al., 2016) and therefore disproportionately high (Dellarocas and Wood, 2008) and not necessarily reflecting solely positive experiences (Bradley, 2019). However, the remaining 5% of ratings which come either in the neutral or negative piles due to delivery problems, scams, or poor quality (Bhaskar et al., 2019) can be leveraged for disruption purposes.

Indeed, it has been shown that both on legal platforms, like eBay, and on Darknet markets, positive and negative reputations do not carry the same weight. While positive feedback drives prices up for vendors (Resnick et al., 2003; Houser and Wooders, 2006; Cabral, 2012), negative ratings not only lower prices but also lower sale numbers significantly (Ba and Pavlou, 2002; Resnick and Zeckhauser, 2002; Cabral and Hortacsu, 2004; Rabby and Shahriar, 2016; Perez-Truglia, 2018; Bhaskar et al., 2019). However, these negative reputations don't necessarily stick because vendors can easily change their identity and therefore have opportunities to misbehave without paying any real reputational consequences (Friedman and Resnick, 2001). Buyers have therefore used positive reputations as a decision-making factor when choosing between different vendors (*Ibid*.). Positive reputations are so important in fact that vendors do not only aim to create 'linkable' accounts across several marketplaces (Soska and Christin, 2015; Broseus et al., 2016), but other vendors also use reputable sellers' usernames on other marketplaces in order to benefit from their standing (Broseus et al., 2016).

Du et al. (2013) have shown that market efficiency is higher when rating information is provided, even if it is unfair or ambiguous, than when it isn't provided at all. Darknet market administrators are aware of this and would therefore not consider removing these mechanisms altogether, so researching this instance would be unrealistic. However, knowing the importance of reputation, these rating mechanisms could potentially be tampered with to drive market failure on Darknet markets, as the trades they facilitate can cause harm.

Understanding the importance of reputation (Lusthaus, 2018), the Police and others have been experimenting with other policing operations in the hope of rendering these Darknet markets less attractive to participants by impacting trust and cooperation. Indeed, sociological research in the past has often focused on the motivations needed to spur cooperation (Williams, 1990). However, cybercriminal traders' self-serving motivations can also break this cooperation and trust down (Morselli et al., 2017), which is of particular interest on harm-causing marketplaces. Indeed, even without the ability to communicate and share reliable information (Campana and Varese, 2013), the absence of official courts to provide protection and after-sale customer service, these markets are still in operation and worth billions of dollars each year. Trust and cooperation are therefore still very much present among Darknet participants (Norbutas, 2020). Can this trust and cooperation be disrupted and lead to Darknet markets' failure from the inside? Two of the most discussed tactics to that effect are slander and Sybil operations.

Slander operations involve users, including the Police and others, creating fictitious profiles and leaving negative feedback to the most honest and successful sellers in order to tarnish their reputation (Mell, 2012). The owner of the fictitious profile only complains that the goods or services they received are poor or fraudulent when they are of good quality. However, the undercover agent makes no complaint if the goods or services received are actually of low quality or fraudulent (*Ibid*.). This should consequently decrease the sellers' potential profits and benefits and increase the perceived risk for buyers wanting to trade with them (Décary-Hétu and Dupont, 2013; Yip et al., 2013b; Decary-Hetu and Laferriere, 2015; Hutchings and Holt, 2017; Paquet-Clouston et al., 2017).

Sybil operations involve the Police and others creating several fictitious profiles, which participate in fictitious transactions together and provide positive feedback to each other,

therefore building up their reputation. However, these profiles are made to default on sales made by non-fictitious buyers (Décary-Hétu and Dupont, 2013; Yip et al., 2013b; Hutchings and Holt, 2017; Paquet-Clouston et al., 2017), therefore undermining the forum's verification system and inciting mistrust among its members.

Both of these operations seek to undermine these marketplaces' trust systems (Mell, 2012; Décary-Hétu and Dupont, 2013; Yip et al., 2013b; Decary-Hetu and Laferriere, 2015; Dupont et al., 2016; Hutchings and Holt, 2017) and build upon the idea to "spoil communication, create distrust and suspicion" (Schelling, 1984, p. 211) within a network, to decrease the amount of illegal trade on these marketplaces. No descriptions of the aftermath of the use of slander or Sybil attacks were found in the literature, however, and researchers who have studied these types of operations have differing opinions about their potential for success. Indeed, while Dupont et al (2016) argue that these operations are not effective as they do not believe they affect the "distribution of trust [they] observed in these forums" due to the networks' resilience to the random loss of nodes, Mell (2012) believes that this method could successfully decrease the number of participants because these markets are sensitive to attacks on their reputational mechanisms. Following a survey of the literature, Bradley (2019) only identified 'parcel seizures' as policing events impacting cybercriminal traders' reputation in a negative way. Slander and Sybil operations might therefore reach such results, as well as creating a 'fear of the Police' and a 'fear of instability', in turn engendering the loss of 'coin', 'products', and 'trading partners' if these conditions are exacerbated, which would eventually lead to a diminished capacity to trade (Bradley, 2019), the ultimate goal in this case.

A range of actors have therefore been identified through this review as participating in the policing of online illegal drug and wildlife trades, including the Police, the legal online platforms these trades happen on, private organisations and individuals skilled in these matters, and cybercriminal traders themselves. As no classification currently exists about the policing of this specific type of cybercrime, this thesis will design its own policing framework building on insights from interviews, content analysis, and laboratory experiments. Later in this thesis, this framework will be evaluated against Button (2019)'s policing classification, one of the most recent policing classifications in the field.

2.4 A classification of policing

Following a recent update to account for the technological evolution of crime and policing, Button (2019)'s policing classification now includes four groups: State Police, Hybrid Police, Voluntary Policing, and the Private Security Industry. As one of the most recent policing classifications, and one that includes a technological component, this framework is described in detail before being compared to this thesis' own policing classification in the Discussion chapter.

Button (2019)'s policing classification is a continuum ranging from public to private policing (see Table 2.1). He argues that rather than being a black and white difference, there exist grey areas between State and Private Policing bodies based on their access, agency, and interest (Benn and Gaus, 1983). As such, access to locations, activities, information, and resources needed for their work can be public or restricted; policing agents can work for the State or act on their own accounts; and their actions can benefit all or serve limited interests (*Ibid*.). In Button's (2019) classification, the State Police is fully public and the Private Security Industry fully private. However, the Hybrid and Voluntary Policing categories in between have various degrees of publicness and privateness, which are detailed further below.

Table 2.1: A classification of policing (adapted from Button, 2019, pp.24)

Category of policing	Examples
State Police Bodies	New York Police Department (USA), Metropolitan Police Service (UK), National Police Agency (Japan)
Hybrid Policing Bodies **State Public Policing Bodies (non-Police)** **Specialised Police Bodies** **NGO Policing Bodies**	 Health and Safety Executive (UK) National Crime Agency (UK), Civil Nuclear Constabulary (UK) Scottish RSPCA (UK)
Voluntary Policing	Paedophile Hunters UK
Private Security Industry	G4S, Securitas, AB, Prosegur

2.4.1 State Police Bodies

First, Button (2019) defines the State Police as a group of professionals employed by the State with a broad mandate for maintaining order and serving the general public for no fee, largely funded by the State, largely uniformed, and holding an office and special set of powers higher than ordinary citizens. Examples of State Police include the London Metropolitan Police and the New York Police Department.

2.4.2 Hybrid Policing Bodies

The Hybrid Police encompasses State and private organisations that do not exhibit all the characteristics of the State Police, as they often have an ambiguous degree of privateness without being commercial or in-house security providers (*Ibid*.). Such a category was already included in Johnston (1992)'s and Jones and Newburn (1998)'s classifications. However, for Button (2019), the Hybrid Police include three groups: State Public Policing Bodies, Specialised Police Organisations, and NGOs.

State Public Policing Bodies are engaged in policing activities as part of the State, mostly involving intelligence gathering and border protection, such as MI6 protecting the State against external threats by collecting and disseminating intelligence to prevent armed conflict, and Customs enforcing border controls and immigration protection (Button, 2019).

Specialised Police Organisations hold comparable powers to the State Police but their specialism in serious crimes, including drug enforcement or transportation, sometimes causes ambiguity over their status. The US Drug Enforcement Agency therefore enforces laws and regulations pertaining to drugs, and the National Crime Agency is the lead UK agency for organised crime in its various forms (Button, 2019).

NGOs are also engaged in policing and are sometimes recognised in law as enforcement bodies, such as the Scottish and New Zealand Societies for Prevention of Cruelty to Animals (SPCA) in their respective countries. Although NGOs were neglected by Jones and Newburn (1998) in their classification, they are very much engaged in policing (Nurse, 2013). Several charity and not-for-profit organisations were cited as specifically policing crimes against animals, which is the prime example Button (2019) uses to illustrate NGO involvement. Crimes

against animals are indeed a powerful example, as these crimes are generally of low priority and few State Police resources are therefore dedicated to enforcing relevant laws (Nurse, 2013). However, these issues are important to large sections of the public, which call for action and make financial donations to external bodies to act on the problem, as shown by the establishment of the RSPCA in the UK even before the London Metropolitan Police (Button, 2019). Their activities include conducting investigations, acting as conduits for complaints from the public, campaigning to expose and end malpractice in their chosen sphere, and training law enforcement in specific issues (*Ibid*.).

2.4.3 Voluntary Policing

Button (2019) then defines Voluntary Policing as tasks performed by individuals and organisations involved in responsible citizenship, which is supported by the State, and autonomous citizenship, which isn't.

Responsible citizenship exists in various forms from individuals volunteering to work as auxiliaries to the Police to helping more informally as bystanders or during one-off missions, such as search parties (Button, 2019). By contrast, autonomous citizenship is not supported by legal authority, and mostly referred to as vigilantism, often conducted with an aim of revenge (Button, 2019). Johnston (1996) defines vigilantism following six characteristics, including some form of planning or premeditation; the use of private voluntary agency, in contrast to Police officers acting off-duty; the lack of support or authority from the State; the use or threatened use of force; the reaction to crime or social deviance; and the contribution to personal and collective safety. Such behaviours are believed to be particularly accentuated by perceptions that the Criminal Justice System is not effective and the awareness of sensational crimes (Button, 2019).

2.4.4 Private Security Industry

Finally, as seen in previous academic literatures, the Private Security Industry is a crucial part of the policing apparatus focussing on the private provision of security and protection (George and Button, 2000). Button (2019) draws a distinction between two types of Private Security Industries – old and new – the former having started before the advent of the Internet and the latter after. Indeed, while staffed security, security equipment, and investigations are still

relevant today, a whole new variety of risks emerged with the Internet (Button and Cross, 2017). This gave rise to new services such as designing, building, and maintaining security systems, threat intelligence, penetration testing, incident response, digital investigation services, disaster recovery, data compliance and protection, and cyber security software products, among many others (Button, 2019). In light of these activities, old and new, it is therefore a misconception that the Private Security Industry does not hold any power. Indeed, although most agents do not have statutory powers, Private Security Industry professionals can secure authoritative powers, including searching, forcible ejection, and interrogation (*Ibid*.). The Private Security Industry as a whole encompasses various levels of employees, from corporate security management, responsible for delivering security objectives, to private security officers, delivering such objectives, as well as specialised roles such as patrolling officers, who patrol their organisations instead of the streets, and private investigators, who conduct inquiries for clients for a fee (Prenzler, 2006).

While remaining statutorily severed from the State and Hybrid Police, Button (2019) argues the Private Security Industry maintains relationships with them, which he categorises in several stages of support from the Police denying their existence and input, to begrudgingly recognising their value, competing with them, calling for their greater control, actively partnering, and equal partnering.

2.5 The gap in the literature and this thesis' research questions

Although many entities are covered in Button (2019)'s policing framework, the policing of online illegal trade is only mentioned in passing as part of the 'new' Private Security Industry, which he argues is necessary to police cyberspace (Button, 2020). Instead, he privileges cyber security specialists who protect private organisations, moderators on social media platforms who remove hate content, and vigilantes who identify scams and paedophiles (*Ibid*.). Indeed, Button (2019) only briefly references NGOs' involvement in the policing of illegal wildlife trade and no mention is made about these trades and policing happening online. However, online illegal drug and wildlife trades have significant adverse effects, the COVID-19 pandemic has increased their volume and value, and there is currently limited academic focus on the policing of these trades. This thesis therefore focusses on how and by whom these trades have been and can be further disrupted. The main objectives of this research are:

1. To identify the policing actors and activities involved in the policing of online illegal drug and wildlife trades;
2. To design a new cyber policing classification and evaluate the relevance of Button (2019)'s policing classification in the context of online illegal drug and wildlife trades;
3. To compare the actors and activities involved in the policing of online illegal drug and wildlife trades;
4. To suggest ways the policing of online illegal drug and wildlife trades could be rendered more collaborative and effective by devising the first 'policing script' summarising the stages involved in these interventions and the actors best placed to conduct them.

In an attempt to address the gaps identified in the literature and to fulfil the objectives of this study, this thesis will aim to answer the following questions:

1. Who is involved in the policing of online illegal drug and wildlife trades?
2. What activities do these policing actors perform?
3. How similar or different are the policing actors and activities involved in the policing of online illegal drug and wildlife trades?
4. How can these types of policing be rendered more effective in the future?

The following chapter details the methods used to answer these research questions.

3 Methods

This thesis used mixed social science methods and triangulated data from different primary and secondary sources. The researcher conducted semi-structured interviews to gather insights about various experts' involvement in the policing of online illegal drug and wildlife trades, as well as performing content analysis on written publications to analyse the way in which several organisations talk about their role in these policing activities. This research project also involved a social laboratory experiment which allowed for the observation of participants' behaviours following trust-related policing interventions.

3.1 Interviews

Details about the interviewing process used to gather qualitative insights for this thesis are presented below.

3.1.1 Sampling

Interviewees were chosen based on their organisation's involvement and expertise in online illegal drug or wildlife trade policing. In the case of wildlife experts, Moshier et al. (2019)'s list of organisations involved in the counter wildlife trafficking community was a good starting point. Drugs being the products sold the most on Darknet markets (EMCDDA and Europol, 2017a), interviewees were able to talk about this trade even if this wasn't their specialism, as they came across these products and traders as part of other investigations. The scope for potential threat intelligence and technology research organisations able to speak to this kind of policing was therefore broader. In both cases, the final sample was dependent on the response from potential participants who were contacted through emails, online forms, or personal contacts, with an average response rate of 41%, 81% of which were positive responses. However, 37% of these respondents eventually stopped answering the researcher's emails during the pandemic, meaning 12 agreed upon interviews were never completed. Several interviewees were introduced to the researcher by previous interviewees, which reached better (though not perfect) response rates. The researcher also met one interviewee at a university event involving alumni. In the case of international organisations, some interview requests were forwarded to experts in other locations than the UK. While the

sample was therefore not geographically-bound, it was limited to English-speaking interviewees.

3.1.2 Topics of discussion

Semi-structured interviews were organised in pre-determined topics of discussion including interviewees' previous and current work and expertise, their organisation's strategy regarding the policing of online illegal trade, any collaborations they have been involved in as part of these activities, and the rules their organisations abide by in their communications, if any (see Appendices A.1, B.1, C.1). The researcher sent these topics to interviewees in advance, due to possible subject sensitivities. However, as these were not fully structured interviews, these topics allowed for some flexibility if some questions were irrelevant or if others were more appropriate in particular cases.

3.1.3 Data collection

20 interviews were conducted between August 2019 and April 2021. The COVID-19 pandemic has rendered data collection more difficult, as interviewees could not be approached at events and conferences and their workloads increased while working remotely. All but one interview were conducted over the phone or through videoconferencing and, with the written consent of interviewees, were audio recorded for more precision during the data management stage. Interviewees' sectors and countries of activity, current positions, and additional logistical information about interviews themselves are provided below. Interviewees' names and organisations are not included, as the topic of analysis is sensitive, but they are referred to with codes based on their activity.

The first group of letters in the below codes indicates the sector of activity of each interviewee: Police (P), Legal Platforms (LP), and Private Organisations and Individuals (POI). The second group of letter indicates whether the interviewee shared insights about drug trade (D), wildlife trade (W), or both drug and wildlife trades (DW).
The final digit in these codes refers to the chronological order of interviews in each category.

Table 3.1: List of Police interview participants

Code	Profession	Country	Date	Type	Timing
P-D1	Detective Sergeant in regional cybercrime unit	England	August 23rd 2019	In person Not recorded	NA
P-D2	Enforcement participant in undercover international Darknet market takedown	Netherlands	November 26th 2019	Video Recorded	39mins
P-D3	Director of prevention policing group	England	March 3rd 2020	Audio only Recorded	40mins
P-W1	Coordinator of online illegal wildlife trade international policy	Switzerland	April 24th 2020	Audio only Recorded	50mins
P-W2	Investigative Support Officer for local wildlife crime unit	England	August 4th 2020	Audio only Recorded	71mins
P-W3	Cybercrime regional programme coordinator for international agency	Thailand	August 5th 2020	Audio only Recorded	54mins

Table 3.2: List of legal online platform interview participants

Code	Profession	Country	Date	Type	Timing
LP-W1	Director of Operations for online pet marketplace	Germany	October 27th 2020	Video Recorded	51mins
LP-DW1	Policy Manager for international online marketplace	United States	April 20th 2021	Video Recorded	64mins

Table 3.3: List of private organisation and individual interview participants

Code	Profession	Country	Date	Type	Timing
POI-D1	Manager of outreach for cyber security research in technology conglomerate	England	November 27th 2019	Audio only Recorded	59mins
POI-D2	Director of research in a cyber security company	England	January 13th 2020	Audio only Recorded	37mins
POI-D3	Intelligence analyst for a non-profit cyber security organisation	England	April 23rd 2020	Video Recorded	46mins
POI-D4	Head of Darknet research for a cyber threat intelligence company	England	May 11th 2020	Audio only Recorded	71mins
POI-D5	Co-founder of digital risk protection company	England	November 19th 2020	Video Recorded	37mins
POI-D6	Director of drug education group	United States	December 18th 2020	Video Recorded	51mins
POI-W1	Convenor of Master programme encompassing wildlife trade	England	February 25th 2020	Video Recorded	58mins
POI-W2	Director of the national branch of an international conservation organisation	China	March 3rd 2020	Audio only Recorded	49mins
POI-W3	Director of a non-profit wildlife forensics organisation	Scotland	April 14th 2020	Video Recorded	54mins
POI-W4	Wildlife forensic expert	Scotland	April 14th 2020	Video Recorded	47mins
POI-W5	Cyber program officer for wildlife welfare organisation	United States	July 13th 2020	Video Recorded	67mins
POI-W6	Senior analyst researching organised crime in an international organisation	Switzerland	December 7th 2020	Video Recorded	41mins

3.1.4 Data management

Personal data was managed systematically, and interviews transcribed within 24 hours of their completion for a better recollection of the words, attitudes, and tones of interviewees. Some interviewees also requested copies of their transcripts and/or quotes used in the researcher's thesis, which therefore also had to be managed on a case-by-case basis.

3.1.5 Data analysis

After transcription, interviews were first pre-coded by highlighting areas worthy of attention (Saldaña, 2016). The interviews were then coded according to themes and theoretical frameworks identified in the Literature review chapter (Miles and Huberman, 1994).

3.1.6 Advantages and Limitations

The use of semi-structured interviews allowed for a greater degree of freedom when asking follow-up questions, requesting additional details, or omitting questions when they had already been answered or were not relevant (Matthews and Ross, 2010). This enabled interviewees to discuss topics the researcher might not have included, sharing their story and experience instead of fitting a prescribed mould. However, semi-structured interviews are not considered as reliable and generalisable as structured ones (*Ibid*.). Indeed, the experiences that interviewees narrated are unlikely to be similar, especially in this context where respondents span different sectors, professions, and continents. However, the purpose of this qualitative research method is not generalisability but the gathering of rich and diverse data. These interviews were therefore deemed most appropriate for this study, which is considered more exploratory, as respondents pointed the researcher in new directions and allowed for the diversification of the initial pool of interviewees in unexpected but insightful ways.

3.1.7 Ethical approval

The aforementioned interviews abided by the University of Oxford Ethics Policy; they did not physically or psychologically harm the interviewees. No research was conducted without the voluntary consent of the interviewees and they were carefully informed about the nature and purpose of the research through an information sheet prior to any data collection. Additionally, interviewees were assured that privacy, anonymity, and confidentiality would

be maintained throughout and after the project and that they would be allowed to withdraw from the study at any point without justification. No respondents withdrew during or after participation. Ethical clearance was received from the Sociology DREC in July 2019.

3.1.8 Reflection on the interview process

From the beginning of the interview process, it was easier to conduct interviews over the phone or through videoconferencing to reach a wider range of interviewees across the world, and even some in London when timings just made travelling inconvenient. The 2020 lockdowns made this strategy essential, as travelling became prohibited and the few in-person interviews that had been organised had to be conducted remotely as well. However, interviews organised over the phone or videoconferencing might have made it more challenging for participants to stay focussed and engaged. Additionally, these remote interviews could also have led to different responses being given than in person, due to a lack of in-person rapport with the interviewer to put them at ease and convey trustworthiness. Some experts were also less inclined to participate remotely due to the sensitive nature of the topics to be discussed, which would have been more appropriate in person. This was particularly the case for legitimate online platform administrators who are the group the least represented in this sample, as only connections of the researcher's contacts agreed to take part in these calls. It is unclear why this group would be less responsive than the Police, who also have to operate with discretion. However, conversations with two platform administrators revealed that they are the first line of defence against illegal trades on their platforms, and they can therefore come under a lot of scrutiny from their users. Many legal platforms which are not up to date on their policies and interventions are therefore reticent to speak about their lack of action, and those which do intervene are still conscious about some of their failures. It is therefore possible respondents declined to participate on this basis.

It is also plausible that interviewees altered their responses knowing they were being actively listened to and (sometimes) quoted. While questions such as 'How long have you been working for the company?' and 'What does your position entail?' all invite simple and (hopefully) honest responses, additional questions about the collaborative work organisations perform with others in the industry or other sectors could have potentially led

to participants embellishing or hiding reality, at the expense of the truth. This might not be the case for certain or any participants, but it is important to note it might be a potential effect of asking questions which, in their eyes, warranted a positive answer. Some, of course, pointed out that they took part in some collaborative work but still needed to do more and are hoping to put more emphasis on that aspect of their work in the future. Others, without being directly asked, expressed opinions about who they would or would not like to work with, which sectors or organisations have or haven't been helpful in this policing, and which ones should stop even trying. Such honesty and criticism were insightful for the purpose of this study and when trying to ascertain how collaborative work in the online illegal trade policing arena currently is or could be happening. However, it might be interesting to ask why interviewees felt they could be so vocal about these issues, as these comments were made by several interviewees – did they feel so comfortable with the researcher that they were able to share their views? Did the 'remoteness' of conversations through audio or video call make these interviews seem less real and their comments less powerful?

As interviews went on, the researcher became more confident in her way of asking questions, for instance repeating a question that had not been fully answered but only circled around, and asking interviewees for contacts in other organisations or sectors, which she did not feel as comfortable doing initially. The power of pauses in conversations also became apparent. Indeed, as many interviews were conducted with no video input, the researcher initially tried to be very reactive when interviewees had finished their answers, so as not to make them feel uncomfortable or to signal that she was still on the other end of the call. As interviews went on, it appeared that short pauses when she was still writing down notes and unable to thank the interviewee for a specific response, comment on their insightfulness, or provide a rebuttal straight away, actually led to interviewees sharing more of their story. Some interviewees became even more open about their circumstances or organisations after having been given more space in these pauses. The researcher therefore learnt to give some interviewees the time they needed to get their story out and quickly reassure others that the technology was still working.

The researcher became able to add more value to interviewees, not only listening to their stories in a one-sided way but having two-sided discussions with them as time went on. She

also became better able to guide the discussion and ask for additional insights as she knew what other interviewees had mentioned in similar organisations, and clarified whether specific activities had been omitted or whether the organisation in question didn't partake in them.

Content analysis was conducted simultaneously in order to gather complementary quantitative and qualitative insights about the ways various organisations talk about their and others' role in the policing of online illegal drug and wildlife trades.

3.2 Content analysis

This project also used content analysis to answer its research questions, defined as "the systematic, objective, quantitative analysis of message characteristics" (Neuendorf, 2016), therefore focusing on the analysis of already-existing data instead of generating new data (Bryman, 2012; Krippendorff, 2013). This research method has been used since the end of the 19th century in order to describe trends in communication content, disclose differences, compare media and/or levels of communication (Berelson, 1952), track discourse and attitudes about specific issues over a period of time (Altheide and Schneider, 2013), and identify thematic patterns within texts and communications (Neuendorf, 2016), all of which are relevant for this study. In its early days, this mostly applied to the study of newspaper content (Berelson, 1952), but for the past sixty years in the fields of journalism, sociology, psychology, and business, among others, it has evolved to other forms of mass communication, such as radio, television, and now the Internet (Neuendorf, 2016). In this age of online communication, reports, press releases, and policies created for the Internet are at the centre of this investigation.

3.2.1 Sampling

Relevance and convenience sampling techniques were employed, therefore encompassing all relevant available textual units from chosen organisations that contribute to answering this thesis' research questions (Krippendorff, 2013). This means texts were examined in advance to ensure their relevance, which is explained further in the Data analysis section below. These texts were also stratified into distinct populations: the Police, legal online platforms, and private organisations.

Specific Police agencies were chosen for this study because they were established agencies possessing both drugs and wildlife expertise. Although specialised agencies exist such as the EMCDDA, the Drug Enforcement Agency, the National Wildlife Crime Unit (NWCU), and the RPSCA, these are not included in this analysis as the aim is to demonstrate non-specialised Police's approach to disrupting both of these trades and to enable comparisons between the two. For this reason and the fact that it is involved in coordinating and advising the update of the Convention rather than purely enforcement-related activities, the CITES Secretariat isn't

included in this analysis either. The chosen agencies also regularly published public reports or news articles either on their own or jointly with other organisations, a significant number of which addressed online illegal drug and wildlife trades and their policing specifically. These agencies also arranged their content in a way that was easy to find and track. Indeed, other organisations which possessed various categories of content that were not well dated and overlapped each other, such as Interpol, were not chosen for this analysis, as identifying all of their related publications was not feasible. Following these criteria, the chosen agencies were Europol, the United Nations Office on Drugs and Crime (UNODC), and the World Customs Organisation (WCO). All of their relevant communications published until the end of the 2020 calendar year were included in this analysis.

Europol is the European Union's enforcement authority, mandated to support national Police agencies throughout the Union and act as a hub for information and expertise to keep Europeans safe from large-scale threats such as terrorism, international human and drug trafficking, money laundering, organised fraud, and money counterfeiting (Europol, 2020b). It was initially established in 1991 as the Central European Investigation Office to fight drug trafficking and organised crime (Europol, 2020c). Europol produces a number of documents each year to keep enforcement, government, and industry partners, as well as the general public, updated on their activities, research, and assessment of future developments and challenges in the threat landscape. A number of documents in the past 16 years have covered online drug and wildlife trades on the surface and Dark web and their policing to some degree. Several of these documents have been written and published alongside the EMCDDA, one of Europol's direct partners for drug trade policing.

The UNODC was established as the Office for Drug Control and Crime prevention in 1997 as a member of the United Nations Development Group and adopted its current name in 2002 (United Nations Office at Vienna, 2020). Despite its name, the remit of the UNODC is wider than drugs, as it also covers topics such as cybercrime, firearms, human trafficking, piracy, and wildlife and forest crime (UNODC, 2020b). Its role is to strengthen UN Member States' capacities to confront threats from transnational organised crime, tackle corruption, strengthen crime prevention, build effective criminal justice systems, and counter terrorism

(UNODC, 2020a). Its publications range from annual reports to bulletins and magazines on specific topics, including annual World Drug Reports.

The WCO was established as the Customs-Co-operation council in 1952 and adopted its current name in 1994 (WCO, 2020c). Its role is to control the international movement of goods, ensuring proper revenue collection, economic interests protection, economic development, societal protection, and security (WCO, 2020b). The WCO is an independent intergovernmental organisation spanning 183 countries and processing approximately 98% of international trade (WCO, 2020e). Its key role is to assist its Members in running their modern Customs administrations by following a set of international rules and standards, building their capacity, and encouraging international cooperation and the sharing of best practices (WCO, 2020d). The WCO regularly publishes short news articles, quarterly news magazines encompassing a range of customs-related issues, illicit trade reports, and annual reports, outlining its recent activities.

A list of the 100 documents published by Europol, UNODC, and WCO which fit this project's criteria is provided in Appendices A.2, A.3, A.4, and A.5. These documents were all public written documents, they were all conveniently presented on the organisations' websites, they all mentioned the policing of online illegal drug and wildlife trades at least once, and they were all published before the end of 2020.

Specific legal platforms were chosen for this study because they were mentioned in Police and other reports as contributing to growing volumes of sales (WJC, 2017b; IFAW, 2018a; WJC, 2018a). They also all boasted trading policies related to drugs and/or wildlife on their sites, as well as some blog posts and reports detailing their progress on this front in several cases. These platforms include general trading websites such as eBay, Etsy, Freeads, and Gumtree, online pet stores such as Pets4Homes and Preloved, social media applications such as Facebook, Instagram, and Twitter, and instant messaging applications such as WeChat and WhatsApp. These platforms were also chosen because they include both sites currently working or having previously worked as part of groups to reduce illegal drugs and wildlife trades online (eBay, 2016c; Facebook, 2018b; Coalition to End Wildlife Trafficking Online, 2020) and others which are not and have not. All of their relevant communications published until the end of the 2020 calendar year were included in this analysis.

44 distinct policies and relevant documents which fit the above criteria were analysed as part of this study, pertaining to both online illegal drug and wildlife trades. These policies and documents are presented in Appendices B.2 and B.3.

Specific private organisations were chosen for this study because they were established companies possessing threat assessment capabilities or conservation organisations with global reach undertaking regular research into online illegal trade and marketplaces. These organisations also regularly published reports or blog posts, either on their own or jointly with other organisations, a significant number of which addressed online illegal drug and wildlife trades and their policing specifically. These organisations also arranged their content in a way that was easy to find and track, unlike TRAFFIC which would also have suited this analysis but for which the content wasn't dated as diligently and involved overlap rendering distinct publications more difficult to identify. Following these criteria, the chosen companies were the Centre for Safe Internet Pharmacies (CSIP), Cyjax, Flashpoint, the International Fund for Animal Welfare (IFAW) and the Wildlife Justice Commission (WJC). As animal welfare organisations published more documents than threat intelligence and education organisations, three organisations are included for the analysis of drug-related documents and two for wildlife-related ones. The inclusion of three organisations publishing drug-related documents also reflects the breadth of organisations involved in this kind of policing, compared to mostly animal welfare and conservation organisations policing online illegal wildlife trade. All of their relevant communications published until the end of the 2020 calendar year were included in this analysis.

CSIP is a non-profit organisation founded in 2011 that aims to promote safe online pharmacies through education, enforcement, and information sharing. The centre includes various organisations such as Internet Service Providers, technology, transport, and payment companies, at the forefront of these issues to address this global problem of consumer access to illegitimate pharmaceuticals (CSIP, 2021a). Together these organisations raise public awareness about the dangers associated with such medications through frequent news and blog updates emphasising the importance of safe online pharmacies (CSIP, 2021b).

Cyjax is a provider of cyber threat intelligence established in 2012 and working to help governments and companies, mostly in the Fortune 500, to build effective threat intelligence

solutions to tackle the digital threats they face (Cyjax, 2020a). The organisation uses its threat intelligence platforms in order to gather data from the surface web, Deepweb, and Darknet, analyse it to identify potential threats, and disseminate the information and actionable points to its clients (Cyjax, 2020b). Cyjax also provides incident response capabilities when an organisation has been affected by a security breach (Cyjax, 2020e). Some of the pertinent insights gathered as part of their monitoring activities are also made available to the wider public, though in smaller quantities, in the form of blog posts (Cyjax, 2020f).

Flashpoint is a provider of cyber threat intelligence established in 2010 and specialising in providing Business Risk Intelligence gathered from the Deep and Dark Webs, as the company argues insights from this hidden part of the Internet are more valuable than other data usually gathered for security purposes (Flashpoint, 2020a). The organisation employs an expert team not only in the field of cybersecurity but also of languages in order to monitor Darknet markets in several countries (Flashpoint, 2020a). As well as keeping their direct clients informed, Flashpoint provides information to the wider public through blog posts, white papers, podcasts, and presentations about different Darknet markets, products, trends, and operations performed in recent years (Flashpoint, 2020b).

The IFAW was established in 1969 as a response to the commercial hunt for whitecoat seals in Canada (IFAW, 2020a). The NGO was qualified as a campaigner according to Nurse (2013)'s policing roles, as it raises public awareness about issues surrounding animal welfare. It has been involved in several projects for the past 50 years, including conservation, disaster response, wildlife rescue, community engagement, policy engagement, and most important for this study, the fight of wildlife crime online and offline (IFAW, 2020b). This issue has been at the centre of many recent publications.

The WJC was founded in 2015 in light of the economic and ecological urgency brought by increasing volumes of illegal wildlife trade worldwide. Its goal is to achieve justice for animals and the communities animal poaching happens in by supporting Police efforts in their policing of transnational organised wildlife crime and in exposing culprits (WJC, 2020a). Although it is not directly named like IFAW, the WJC fits Nurse (2013)'s definition of the NGO enforcement role, as it actively ensures laws are enforced and investigates those who break them. The Commission regularly undertakes undercover operations to gather evidence against specific

criminal networks and provides this information to the relevant government and enforcement agencies (WJC, 2020b).

A list of the 58 documents published by CSIP, Cyjax, Flashpoint, IFAW, and WJC which fit our criteria is provided in Appendices C.2 and C.3. These documents were all public written documents, they were all conveniently presented on the organisations' websites, they all mentioned the policing of online illegal drug and wildlife trades at least once, and they were all published before the end of 2020.

3.2.2 Data management

An index was initially devised in order to gather basic information about each document in its totality and create an overarching view of texts before focussed analysis. This index included categories such as the title of the document, its type, its intended audience, the sector of its author(s), their location, its publication year, its overall theme, its specific focus, its content type, its format, and its length. This index was filled in progressively as each document was reviewed.

3.2.3 Data analysis

There is no 'right way' to perform content analyses and to design coding schemes (Weber, 1990), as they are largely dependent on the content for review and goal of the analysis. Based on several prescriptive flowcharts in the content analysis literature (Weber, 1990; Schreier, 2012; Altheide and Schneider, 2013; Neuendorf, 2016), the following protocol was followed in order to perform this content analysis based on the best identified practices for this research method: 1) the theory and rationale for the study were defined, including the content of interest and research questions to be answered, 2) the data sources were examined and chosen in order for the researcher to become more familiar with their context, 3) coding units for analysis were defined, 4) keywords for counts and categories to be analysed were defined, 5) a manual keyword and category count was performed on a small representative sample of Police, legal online platform, and private organisation documents, 6) a manual coding analysis was performed on a small representative sample, 7) the coding rules were revised, 8) keyword and category counts were performed on the entire sample, 9) the entire sample was manually coded, 10) paragraphs were analysed qualitatively in order

to gather more data about the context of the keywords and categories of interest for more in-depth interpretation, and 11) the final results were interpreted and reported. More information about the main steps of this analysis is presented below, including unitising, keyword and category counts, manifest content analysis, and latent content analysis.

Unitising was first performed. Several units of analysis were devised for the above samples: entire documents were used as sampling units - large units distinguishable for selective inclusion - and context units - units of text setting limits on the information to be considered in the description of recording units. Paragraphs were used as recording units - small units distinguished for coding (Berelson, 1952; Krippendorff, 2013).

Keywords and categories were then counted. All analyses started with identifying and quantifying the use of certain keywords and categories to explore their usage in different documents and sectors, and to understand their contextual use.

A manifest content analysis (Potter and Levine-Donnerstein, 1999) was then performed, focussing on what was easily observable on the surface of the sampled documents. In order to better understand how various organisations talk about online illegal drug and wildlife trades' policing to their clients and the wider public, a specifically-designed coding scheme was applied to the reviewed documents. This scheme included the depth of online trade policing mentions, the type of policing mentioned, the status of these operations, the policing collaborations involved, and the role of specific actors in this policing. These categories were unidimensional, only capturing one aspect of material; saturated, leaving no categories unfilled at the end of the analysis (Bryman, 2012; Schreier, 2012); and mutually exclusive (Weber, 1990). However, certain categories were likely to solicit several responses, as some sentences and paragraphs covered much information about the type of policing under scrutiny and disrupters' role in this type of policing. The same coding scheme was systematically applied to every unit of analysis (see Appendices A.6, B.4, C.4). This scheme aimed to describe manifest characteristics of communications, including what is said, how, and to whom, to make inferences about antecedents of communications, why it is said, and about the potential consequences of communications, with what effects things have been said (Holsti, 1969). These goals were fulfilled by using both quantitative and qualitative operations on text (Weber, 1990).

Latent content analysis was consequently performed to conduct an overall summative analysis (Hsieh and Shannon, 2005) by analysing content (Holsti, 1969) and discovering underlying meanings (Babbie, 2016; Bengtsson, 2016). This analysis was based on a common qualitative framework employed in the literature, consisting of 1) identifying meaning units, 2) condensing them into shorter units while preserving meaning, 3) coding them, 4) assigning them to categories of related codes expressing manifest content such as who, what, when, or where, and 5) assigning them to themes expressing underlying meanings in several categories to answer the questions why, how, in what way, or by what means (Erlingsson and Brysiewicz, 2017).

Overall, the above analysis only involved written public communications about online illegal drug and wildlife trades. Some, if not all, of the organisations included in this study also released private reports to specific stakeholders, including their clients or policymakers, which were not publicly available and therefore not included in this study. Additionally, some organisations also provided audio and video content, which was not included for this project as it wasn't universally available for all of the chosen organisations. Some of the keywords used to describe policing interventions such as 'arrest', 'remove', and 'block' were sometimes used in different contexts than the ones of interest for this analysis. Only relevant uses of these keywords were therefore included in the relevant counts. Keywords used in titles, tables of contents, footnotes, or references were not taken into account either, focusing the analysis solely on the direct content of these documents. Additionally, when keywords were counted for various types of operations, only the number of keywords used were reported, rather than the amount of takedown or seizures mentioned in these publications, as the language rather than the volume was of interest for this analysis. In the case of trading policies, only paragraphs and bullet points directly relating to illegal drugs and wildlife were included in the analysis – alcohol and tobacco products often included with drugs were taken out of the analysis, and live non-protected animals and their parts were also discarded. Additionally, only prohibited and restricted items were included in this analysis, so mentions of items allowed on these legal platforms were removed. Finally, only platforms' general policies were analysed, as they were aimed directly at individual and business users, instead of their advertisers, for instance.

3.2.4 Advantages and Limitations

Content analysis was deemed beneficial for this project, as it made use of vastly available communication data to be analysed in a scientific manner, while limiting any personal biases and intrusion from the researcher (Webb, 1966; Krippendorff, 2013). This study is also replicable based on its objectivity, the fact that coding rules and categories were clearly set out, made transparent before the analysis began, and consistently and systematically applied (Bryman, 2012; Krippendorff, 2013). The use of both quantitative and qualitative analyses is also considered positive as it allowed for the gathering of complementary insights not usually obtainable with other research methods (Weber, 1990). This ensured that the context of the keywords and categories of interest were not lost and did not restrict the extent of the analysis (Morgan, 1993), especially in an exploratory study such as this one where little, if any, theory about different sectors' communications about online illegal trade policing was available. However, this method has been criticised for the time-consuming volume of data it engenders for review, including how to access, retrieve, and store original communications, as well as relevant counts and categories (Altheide and Schneider, 2013), which could render the process mindless (Weber, 1990). By including all relevant available data from selected organisations instead of randomising these choices, the study was not only able to evaluate trends overtime, but it also limited the incompleteness of its data (Munksgaard and Demant, 2016). However, certain relevant documents might not have been released, been kept for private audiences, or might have been taken down before this analysis started. Qualitative content analysis has also been criticised for stripping initial communications from their complex, holistic, and context-dependent meanings (Schreier, 2012), which contextualisation within broader units of analysis and across several sectors in a period of time has tried to mitigate. Issues of validity have been brought to the fore (Berelson, 1952) in both cases, as the classification procedure must ensure the variables generated are valid, they measure what the investigator intended to measure and the words used to describe units and categories do no possess similar ambiguous connotations (Weber, 1990). In this context inter-coder reliability, the ability for several coders to reach similar results (Neuendorf, 2016), could not be achieved as the researcher was the sole coding scheme designer and implementer for the project. However, every step was taken to ensure that the scheme was designed

objectively and using clear unit and category definitions so that other coders would have ideally agreed with its application and reached similar results in different contexts.

This study was based on a small number of mostly EU- and US-centric organisations to assess the content of their written public communications regarding the trade of illegal drugs and wildlife online. The findings might therefore not be directly generalisable to other organisations or other continents. The study could however be replicated with other organisations in other countries, or for other types of illegal trade, such as firearms or stolen financial information. The study could also be replicated with other types of data, including audio and video resources which some organisations provided and which might cover different aspects of illegal trade policing than written reports. It should also be noted that all of the organisations included in this analysis come with their own ideologies and goals. Police and Customs agencies, such as Europol, UNODC, and WCO, have a duty to report on their progress and potentially raise awareness about certain types of crimes. Legal trading, social media, and instant messaging sites, such as eBay, Etsy, Facebook, Freeads, Gumtree, Instagram, Pets4Homes, Preloved, Twitter, WeChat, and WhatsApp, need to show their commitment to reducing illegal trade issues on their platforms. Non-profit organisations such as CSIP, IFAW and WJC support the causes of illegal drug use reduction and animal welfare, so their publications could be seen as non-objective. This analysis therefore did not focus on the tone of language used in these publications, as it can be argued to be more passionate and pressing than that of enforcement organisations. The analysis instead focussed on the facts they reported. Similarly, private organisations such as Cyjax and Flashpoint sell a service. While their blog articles are accessible to anyone, interviewees reported they were a good way to get clients through the door. Consequently, these organisations' goal of business development, alongside raising awareness, is argued to be on par with non-profit organisations' passion for their cause, and neither type of organisation can therefore be considered as objective.

3.2.5 Ethical approval

Unlike research performed on social media and Darknet forums, the analysis of Police and other organisations' documents is based on intentionally public material (Wright, 2018). Indeed, even if the earliest relevant documents available date back 15 years, the agencies and

organisations who posted these documents online consented to them being available to the public. Only documents readily available on the relevant websites were included in this analysis and no private or unintentionally public documents, posted online while intended to remain private, were sought to complement these insights. As such, it is understood only non-sensitive data could be shared in these publications, so it was essential to combine these findings with expert interview insights for this thesis.

3.2.6 Reflection on the content analysis process

The researcher had never performed content analysis before conducting research for this thesis. She therefore read about this method, how it had been used in the past, what it allows for, and any best practice in the field. She then took her time experimenting with it for this research which was more exploratory. Indeed, policing communications on this topic have not been analysed in this way before and, being numerous, the researcher initially took months to select organisations of interest, create a broad coding scheme based on categories she had observed during her initial readings, and ensure she counted keywords and categories as objectively as possible. Going through these various pieces, she wrote about each organisation individually as she finished her analyses and created as many graphs as possible to represent the information in different ways. Content was then brought together when analyses were performed on all Police wildlife documents, for instance, writing a general document presenting findings about this specific group and theme, before writing a general Police chapter also including drug findings. This iterative process allowed for content to be reviewed as it was merged with other documents. Taking this exploratory approach therefore allowed the researcher to familiarise herself with this new method by spending more time with each document and analysing many more features than would ultimately be needed. It also ensured that the most salient points were the ones presented in the relevant chapters, as many others did not turn out to be as insightful or in line with the final aim of the study.

Finally, a social laboratory experiment was conducted in order to gather information about an unexpected policing actor – cybercriminal traders themselves.

3.3 Social laboratory experiment

Finally, the researcher conducted a social laboratory experiment to test participant behaviour and decision-making following slander and Sybil interventions, to show the consequences of these Darknet market interventions on cybercriminal traders' behaviours.

3.3.1 A change in research methods

Contrary to the other empirical chapters in this thesis, the chapter about cybercriminal traders does not use interviews and content analysis to determine cybercriminal traders' role in the policing of online illegal drug and wildlife trades. Indeed, data of this form would not only be complex to gather, especially during the pandemic in the case of interviews, but it also would not answer the questions this research seeks to address. Interviews with ex-cybercriminal traders who performed scams or exit scams, if they can be located and agree to participate, would not speak to the impact of their actions on the marketplace but to their motivations. Additionally, content published online by cybercriminal traders performing these actions, or others impacted by them, would not serve the same purpose as Police, legal online platform, and private organisation documents aiming to inform the public objectively, but instead would likely take the form of complaints or warnings, which are not relevant in this case. However, research about issues of interest can be conducted in another way.

Although the Police have been able to infiltrate Darknet markets, it is more complicated for researchers in academia to do so. Indeed, showing the necessary trustworthiness, technical abilities (Lusthaus, 2012; Dupont et al., 2016) and "credibility" (Leukfeldt et al., 2016a) to be accepted as part of such a criminal network might involve taking part in criminal activities, including selling illicit goods or services. Ethical questions could also be raised about researchers manipulating users' rating information, for instance. A social laboratory experiment was therefore conducted for this study as it allowed for a scientific evaluation of market consequences following specific interventions, which in turn informs us about their disruptive potential.

3.3.2 What are social laboratory experiments?

Experiments have been consistently used in the social sciences since the 1960s. Like better-known natural science or medical experiments, social experiments aim to measure the effects of a treatment on a group of human subjects compared to another group subjected to a control, observing what would happen to a given person in a state where they would receive a treatment and one in which they would not (Heckman and Smith, 1995). However, in the case of social experiments, the treatments researchers are measuring the impact of in these controlled environments are in the realms of psychology, economics, or even policy (Rivlin, 1974). Social experiments are often performed in the field, measuring the effects of an intervention on an individual or household while they lead their normal lives but being subjected to a specific intervention, and eventually compared to another group of individuals or households not subjected to it (Greenberg and Shroder, 2004). However, in some cases, such impacts cannot be studied in the real world and instead require a laboratory setting, as was the case for this experiment. While Darknet markets do exist in the real world, conducting experiments on them, as well as being unethical for a range of reasons such as impersonating cybercriminal traders and tampering with vendors' reputational ratings, would not satisfy the controlled scientific environment needed to measure the impact of a single independent variable on participants. For this experiment, human participants were therefore invited to a computer laboratory where they took part in the experiment together under scientific conditions that had been designed specifically for this purpose.

3.3.3 Experimental design

Social laboratory experiment participants were chosen from a pool of student participants who signed up to participate in CESS experiments. The participants were physically present in Oxford in order to attend the laboratory sessions, over 18 years of age, and spoke English fluently. The slots were attributed on a first-come first-served basis.

The design was created for 144 participants spread over six sessions (two sessions per treatment), as the CESS laboratory can house a maximum of 24 participants at one time. However, the second Control session only accrued 18 participants, leading to a total of 138 participants. This discrepancy is accounted for in the Cybercriminal traders chapter analysis.

As is standard experimental practice (Webster and Sell, 2007) and CESS protocol (CESS Nuffield, 2019), participants were paid for their involvement at an average rate of £10 per hour, with components of this payment built into the games as incentives. Participants were therefore rewarded for their decisions in the experiment, mimicking the profit-seeking behaviour of cybercriminal traders, as it was assumed the aim of each participant was monetary (Von Neumann and Morgenstern, 2007).

All participants were Oxford University students, with no local citizens involved in order to keep the sample homogenous, which is common practice at CESS and elsewhere (Davis and Holt, 1993; Friedman and Sunder, 1994; Levitt and List, 2008; Hooghe et al., 2010). Within the sample, 54% of participants were women and 46% men; 54% were currently involved in undergraduate studies, 19% in taught graduate programmes and 27% in research graduate programmes; 42% studied Social Sciences, 38% Science and Medicine, and 20% Arts and Humanities (see Appendix D.5). The sample is therefore considered representative of the University student population sample the researcher wanted to investigate.

Each participant only took part in one of the experimental treatments, rendering the measures independent rather than repeated (Field and Hole, 2003). Although, it is noted that this between-participants design is less sensitive than repeated measure within-participants designs when detecting effects of experimental manipulations due to random variability between participants, this design's avoidance of fatigue and carry-over effects (*Ibid*.) outweighs these limitations. Indeed, participating in several subsequent treatments might affect participants' behaviours and choices as they are already familiar with the aims of the games and have already participated in several trading rounds, therefore impacting their enthusiasm for and instincts in the games in within-participants experimental designs. Variations in participants preferences and behaviours between treatments are discussed in the Discussion section of the Cybercriminal traders chapter.

3.3.4 Pre-testing and piloting

The experiment, before being conducted with official participants, was first pre-tested and piloted. Pretesting involved reviewing individual experimental tasks in order to get feedback from third parties, while piloting involved conducting complete experimental sessions with

participants acting as informants (Webster and Sell, 2007). For this project, pretesting consisted of presenting an individual experimental game, the reputational "market for lemons" as well as participant instructions, at a CESS seminar session in Trinity Term 2019, in order to get feedback from other experimentalists at the University. Piloting was then conducted in Michaelmas Term 2019 with Centre for Doctoral Training in Cyber Security, Department of Sociology, and St Cross College colleagues who had heard about these experiments in class presentations and other discussions and were eager to see the finished product and give constructive feedback. These sessions were not remunerated as participants understood what the experiment involved. This process was invaluable in testing the experiment in real time and spotting errors in the instructions.

3.3.5 Coding

The oTree framework (Chen, 2019) was used to implement the computer laboratory interface with which the participants interacted. This framework, implemented in Python, is intended for the construction of computer applications for behavioural experiments and multiplayer strategic games, as well as surveys and quizzes. oTree was therefore ideal for the purpose of this study, as the framework provided a full end-to-end toolkit, handling the underlying logic and implementation of the games; the design, layout, and presentation of the user interface through which the participants interacted; the monitoring and processing of participant inputs; and finally, the capture, recording, and basic processing of the raw experimental data.

The games used in the study consisted of modifications to basic oTree templates for the trust game, "market for lemons", and questionnaire already provided by Chen (2019). The modified "market for lemons" game included a sending decision for vendors and rating system for buyers, as well as slander and Sybil interventions, randomly 'compromising' these sending and rating decisions. Other modifications included changes to the information presented to the participants over the duration of the experiment, such as vendors' averaged ratings throughout rounds. Further details about the experiment design are presented in the Cybercriminal traders chapter.

3.3.6 Data management

The experiment was conducted within one week in Michaelmas Term 2019. Personal data about the participants and their individual payments were recorded systematically after each session, in order to keep detailed accounts of these personal details and transactions. Decisions made by the participants throughout the experiment and their survey answers were also recorded and formatted in a convenient manner after each session, as the outputs were presented in a very crude way and it was easier to do these menial tasks every day rather than at the end of week. However, these data were only analysed after all the experimental sessions had taken place, to avoid any bias from the researcher and to avoid omitting any outliers that might have occurred in the last few experiments.

3.3.7 Data analysis

Descriptive statistics were first used on the data and graphs were drawn to visualise the experimental results. Prices and quality measures were collected throughout the experimental sessions and analysed using Kruskal-Wallis and Mann-Whitney U Tests – the non-parametric equivalents of one-way independent ANOVA and independent t-tests. The former is used to test differences between more than two groups involving different participants (Field and Hole, 2003), however this test only shows whether a difference exists between the groups, not where this difference lies. The latter test was therefore used if a difference was noted to test variations between two specific groups of different participants (*Ibid*.). A Bonferroni correction was applied to these subsequent tests in order to limit the potential of Type I error (the conclusion that there is a difference when there isn't). Indeed, Kruskal-Wallis tests include adjustments to ensure Type I errors do not build up to more than 0.05. However, these controls are not in place when performing several Mann-Whitney tests and the 0.05 critical value therefore needs to be divided by the number of tests conducted, in this case three, so the level of significance reported in the Cybercriminal traders chapter is 0.0167. Data about product ratings and decisions to send or not to send products were solely used in order to understand their impact on prices and quality measures, as they were manipulated throughout the experiment, and are not analysed for this study. These tests were used to analyse these experimental results as the gathered data are not parametric – although the data are continuous, the conditions do not have equal variances, and the data

are not normally distributed (all three parameters need to be met for the data to be considered parametric). Such non-parametric tests do not use raw scores but instead rank the data from low scores to high ones. This reduces the amount of information about the magnitude of differences observed and therefore means non-parametric tests are less powerful than their parametric counterparts in their ability to find effects that genuinely exist. This gives an increased chance of Type II error (the probability of accepting there is no difference between groups when there is). Groups are then compared based on their mean rank, the lowest mean rank meaning lower scores than the other group (*Ibid*.).

The formula to calculate the Kruskal-Wallis H statistic is:

$$H = \left[\frac{12}{n(n+1)}\sum_{j=1}^{c}\frac{T_j^2}{n_j}\right] - 3(n+1)$$

Where: n is the sample size for all group, c is the number of groups,
T_j is the sum of ranks for the j^{th} sample, and n_j is the size of the j^{th} sample.

The H statistic is then compared to a critical Chi-Square value calculated based on the relevant degrees of freedom and level of significance desired to determine where a difference exists between groups (*Ibid*.). The null hypothesis of no difference between groups is rejected if the critical Chi-Square value is smaller than the H statistic. Otherwise there is not enough evidence to suggest the groups are unequal. These calculations were performed using Excel and SPSS for this experiment, the latter which also readily provided the significance of the results. H statistics are provided for each of the Kruskal-Wallis tests performed, although their order of magnitude varies significantly as these values take into account sample sizes. However, the critical Chi-Square values are not provided in the Cybercriminal traders chapter, as the sample sizes consistently surpassed those contained in value tables and the software did not provide these numbers before recommending to reject or retain the null hypotheses. Where differences were found, Mann-Whitney U statistics were then calculated to pinpoint which groups differed.

The formulae to calculate the Mann-Whitney U statistics are:

$$U_1 = n_1 n_2 + \frac{n_1(n_1 + 1)}{2} - R_1$$

$$U_2 = n_1 n_2 + \frac{n_2(n_2 + 1)}{2} - R_2$$

Where: n1 and n2 are the sample sizes of each group
and R1 and R2 are the sum of the ranks of each of the values in their group

The smallest U statistic is then compared to a critical U statistic (just as comparisons are done for t-tests with p-values, measures of the probability that an observed difference could have occurred by random chance) to determine the significance of the results (*Ibid*.). The null hypothesis of no difference between groups is rejected if the critical U statistic is larger than the U statistic. Otherwise there is not enough evidence to suggest the two groups are unequal. These calculations were performed using Excel and SPSS for this experiment, the latter which also readily provided the significance of the results. U statistics are provided for each of the Mann-Whitney tests performed, although their order of magnitude varies significantly as these values take into account sample sizes. However, the critical U statistics are not provided in the Cybercriminal traders chapter, as the sample sizes consistently surpassed those contained in value tables and the software did not provide these numbers before recommending to reject or retain the null hypotheses.

Although it was not possible to estimate the power from such statistical testing before the data were collected and analysed, the researcher believed an indication of statistical significance, even at a low power, could confirm her hypotheses and spur future research based on the direction of the findings. The analysis was based on a Type I error of 0.05, giving a 5% probability of rejecting the null hypothesis when it is correct. Based on this choice, it appeared the power of the analysis (the probability of rejecting the null hypothesis when it is false) was higher than initially anticipated with these conversative tests and these numbers therefore warranted inclusion. Indeed, Gallo et al. (2019) noted that any statistically significant findings using non-parametric tests on small samples denote a sizeable treatment effect.

It should be noted that the use of Kruskal-Wallis and Mann-Whitney U Testing in this case could have been impacted by variability between participant groups, as trios were re-allocated after each game. The differences the tests associated with each treatment might therefore stem from participants' varying behaviours in different trios, although these exact variations could not be tested and confirmed. To counter this issue of constant group re-allocation, simple or multiple linear regression could have been performed using one or several independent variables to explain or predict the outcome of a dependent variable when analysing these results. However, such regressions assume data are normally distributed (Olive, 2017), which is not the case in this experiment. Indeed, statistical testing does not fit experimental circumstances perfectly, any assumptions made and potential problems identified therefore need to be clearly laid out for the analysis to be viable. In the case of this low sample size experiment, it was clear the data were not normally distributed. Statistical testing is usually reserved for experiments with larger sample sizes; Fudenberg et al. (2012), Arechar et al. (2017), and Gallo et al. (2019)'s designs adding noise in experiments replicating cooperation situations other than markets, as discussed in the Cybercriminal traders chapter, each involved more than 300 participants, for instance. However, Bolton et al. (2004) conducted a market experiment similar to this project with 144 participants consisting of 30 trading rounds and performed t-tests on their parametric data. Kruskal-Wallis and Mann-Whitney U Tests were therefore performed in this non-parametric experimental context, as it is recommended for this type of between-participant experiment (Field and Hole, 2003).

3.3.8 Advantages and Limitations

Social laboratory experiments were chosen for this study because they offer both replicability and control. Indeed, by providing detailed experimental proceedings, other researchers will be able to reproduce experiments in different locations and with different participants (Davis and Holt, 1993), potentially even including former offenders, in order to verify the findings independently. Additionally, the researcher was able to manipulate laboratory conditions to observe their effects, which is not possible in the natural world, therefore allowing the evaluation of single causes independently to test hypotheses (*Ibid*.). Finally, the proposed treatments contained very similar scenarios, therefore establishing some internal validity for

the study, ensuring that variations in dependent variables were produced by changes in the independent variables and not by 'hidden factors' (Brewer and Crano, 2014) stemming from discrepancies in the study.

This experimental method has, however, been criticised because the undergraduate students who comprise most subject pools for laboratory experiments are not as sophisticated as real decision-makers, therefore creating a lack of generalisability of the findings (Davis and Holt, 1993; Levitt and List, 2008; Hooghe et al., 2010). Additionally, the Hawthorne effect can be argued to play a role in the obtained results, as participants know they are observed and might therefore perform differently than they would in real life (Levitt and List, 2007). The incentive to act like a fairer trader was hopefully offset in this experiment by the monetary incentives associated with malicious behaviour. The possibility to control conditions in this environment has also been deemed too simple to replicate complex markets and other economic environments (Davis and Holt, 1993). Indeed, many economic decision-makers take more time to reach decisions than the typical time limits in a laboratory or online session, and they will often talk to each other before making these decisions, while communication is prohibited during these experiments (Reiley, 2015). This experiment also simplified the Darknet environment in question by creating a duopoly based on an already-established economic game and not incorporating specific aspects of these marketplaces, such as the consistently high ratings, to test a neutral market upon which operations are performed. In the case of online illegal trade, the risks are also more real in actual trading forums compared to fictitious forums, with traders dealing in thousands of dollars instead of matchsticks, meaning participants might not behave as they would in the real world where they could lose a significant amount of money or risk arrest. However, if theories fail to work in environments as simple as these, there is little expectation that they would actually apply in more complex real-life situations (Davis and Holt, 1993), making social laboratory experiments viable options in this case.

3.3.9 Ethical approval

The aforementioned experiment abided by the University of Oxford Ethics Policy. Research conducted for the purpose of the study did not physically or psychologically harm participants. No deception was used for the purpose of this experiment. No research was

conducted without the informed voluntary consent of the participants. Additionally, participants were assured that privacy, anonymity, and confidentiality would be maintained throughout and after the project and that they would be allowed to withdraw from the study at any point without justification. No participants withdrew during or after the experiment. Ethical clearance was received from the CESS in April 2019, as is necessary before running any experiment, and from the Sociology DREC in July 2019.

3.3.10 Reflection on the experimental process

As the first experiment run by the researcher, this research method involved a steep learning curve. Aware of this limitation, the researcher signed up to various courses about the design and conduct of experiments and had lengthy discussions with experts at the CESS to get their input and feedback about her ideas. She also assisted a few experimentalists at the University who were running their own experiments at the Centre to get a better understanding of experimental logistics from the researcher's perspective, to complement the understanding she had previously gathered about experimental structure and functioning as a participant for other CESS experiments.

The experiment also required communicating more extensively with the researcher's supervisors and experimental colleague in Cambridge to inform them about experimental choices and obtain feedback. Although the initial plan was to perform a full experiment, and further funding was obtained for this, the time and effort required for this project rendered a pilot a more viable option for inclusion in this thesis, especially as the pool of participants at the CESS was too small to allow for a bigger study. However, thought was put in ensuring the pilot experiment would engender enough data, as pilot studies do not usually comprise of hundreds of participants. In this case, the experiment therefore lies between a pilot and a full experiment in terms of sample size. This allowed the researcher to test her hand at analysing these results, not only cleaning the data which came out in a very rough format, but also applying statistical tests, not often performed on small sample sizes, to grow as a researcher and analyst by completing this project from start to finish. Indeed, in order to understand the steps involved in these tests, she first performed them by hand on smaller samples of data using Excel before using the SPSS software to compare the thousands of data points gathered for each parameter of interest during the experiment.

The researcher was also given the chance to present her experimental design at the Economic Science Association European conference in September 2019 and her findings at the Oxford University Extra-Legal Governance seminar series in May 2020. These not only furthered her presentation and communication skills, having to present the latter virtually, but also allowed for comments from other researchers and experimentalists in Sociology, Economics, and beyond. Finally, the Cybercriminal traders chapter was the first one the researcher submitted for publication as a journal article, and therefore gave her a better understanding of the peer-review publication process and the aims of different journals, workshops, and conferences.

3.3.11 Co-authorship

The Cybercriminal traders chapter involved the participation of the researcher's supervisors, Dr Jonathan Lusthaus and Prof Federico Varese, who were responsible for securing funding and for the initial idea of bringing social laboratory experiments to the field of cybercrime, and of an experimentalist, Prof Edoardo Gallo from the University of Cambridge who advised about technical aspects of the project. However, the researcher was the one to follow experimental training, liaise with the Nuffield College CESS laboratory, decide on the details and interventions to be included in the experiment, design it, run it, analyse the results, and write them up in the Cybercriminal traders chapter. The researcher is the sole author of this chapter, which is significantly different from the article submitted for publication with the above co-authors.

Experimental coding was attempted by the researcher and her modest knowledge of the Python coding language over the summer of 2019. However, due to time constraints experimental coding was ultimately completed by one of her CDT colleagues, Sean Sirur, in the Department of Computer Science. The relevant co-authorship form has been signed by all of the above parties and submitted to attest to this.

The following four empirical chapters present the findings and analyses from these interviews, content analyses, and social laboratory experiment.

4 The Police

Drugs and related products now constitute two thirds of all traded products on Darknet markets (EMCDDA and Europol, 2017a). They are also increasingly traded on the surface web (Babb, 2014; Thanki and Frederick, 2016; EMCDDA and Europol, 2019; Moyle et al., 2019). While illegal wildlife species and products are not widely available on Darknet markets (Harrison et al., 2016; Cugniere et al., 2019; Wright, 2019), up to 80% of this online trade might now be happening on social media platforms (Krishnasamy and Stoner, 2016), freely and easily accessible by many across the world (IFAW, 2018a; WJC, 2018a; TRAFFIC, 2019), and therefore representing another enforcement challenge (Martin et al., 2018b).

Drugs and wildlife are similar in many respects. However, drugs were extended a priority policing status by the Police long before their sale began on the Internet, and they are the illegal product that has received the most attention related to its Internet-mediated trafficking (Lavorgna, 2014a). Wildlife species and products are just now starting to be referred to by the Police as a mild threat (Europol, 2017g) following years of lobbying from animal welfare organisations, and they have not yet been offered the same extensive Police commitment (South and Wyatt, 2011). We therefore have much to gain from researching both of these products as part of the same study, gathering complementary insights to provide useful strategies for their future individual policing. The activities of the Police in both realms are explored and compared in this chapter.

The aim of this study is to understand how the Police contribute to the policing of online illegal drug and wildlife trades to better situate this group in the cyber policing classification and policing script devised in the Discussion chapter.

Research for this chapter was conducted by analysing the content of 100 publications from Europol, UNODC, and WCO, as these organisations all deal with and communicate about both online illegal drug and wildlife trades, and by interviewing six Police officers in local and international agencies.

This chapter therefore focusses on the Police while investigating this thesis' broad research questions:

1. Are the Police involved in the policing of online illegal drug and wildlife trades?
2. What activities do the Police perform?
3. How similar or different are the Police actors and activities involved in the policing of online illegal drug and wildlife trades?
4. How can this type of policing be rendered more effective in the future?

In order to answer the aforementioned questions, this chapter is divided in three parts, each one focussing on different research questions. The first part presents findings about the Police agencies involved in the policing of online illegal drug and wildlife trades; the second part then analyses the activities the Police perform and how these differ between the policing of online illegal drug and wildlife trades; and the third part discusses how the Police can be more effective in this type of policing in the future.

4.1 Police actors

The Police is used in a broad sense in this project, encompassing local, national, and international agencies working on general enforcement duties or specialising in drug or wildlife crime, as well as agencies working on legislative and preventive activities. Although the Police are the only entity to possess powers such as search and arrest in the public sphere, these agencies do not possess the necessary capabilities and resources to tackle these online illegal trades alone (POI-D4). Police agents' responses varied, when asked about their capabilities with regards to online illegal trade policing. Indeed, local agents recognised their limited capabilities and need to learn from others and receive further training (P-D1). However, international agents were very confident in their capabilities and deemed themselves "*quite well on track*" (P-D2). These assessments therefore show the amount of skills and resources available at different levels.

Specialised units were set up to compensate for these varying levels of skills and resources, especially in the case of illegal wildlife trade for which the lack of relevant knowledge in local and national forces can be glaring:

> *"We're primarily an intelligence and analysis unit, but it was quickly realised at the very start that we needed to have some sort of ability to assist on the ground with investigations because there is a level of knowledge in activities among officers which is quite poor really, they just don't understand a lot about wildlife. […] A lot of what we do involves the trade, you know, it involves CITES, because although a lot of police officers might know about poaching or prosecution offenses, they don't really know about the international trade side." (P-W2)*

The sample of interviewees and content analysis documents for this project therefore show the breadth of agencies and specialisms involved in this type of policing. The answer to our first research question is therefore that a range of Police agencies are involved in the policing of online illegal drug and wildlife trades, including national and international forces, as well as specialised groups working on drug and wildlife issues, and agencies working on broad-ranging issues. The Police is therefore the first part of the cyber policing classification devised in the Discussion chapter. However, the activities they perform overall remain broadly similar.

4.2 Police activities

Insights from interviews and content analysis have highlighted four main activities performed by the Police to disrupt online illegal drug and wildlife trades: 1) Intelligence and expertise receiving, 2) Information gathering, 3) Operation conducting, and 4) Reporting. These are analysed in turn and the specific activities involved in policing both products are emphasised where they differ.

4.2.1 Intelligence and Expertise receiving

In this field, it is important for the Police not to act alone but to receive as much information and expertise from as many other organisations as possible. The reason for this is that they need to have a picture as complete as possible about a cybercriminal trader to bring a successful case to court (P-W2). Such information can include any previous or current trades cybercriminal traders are associated with, their volume, value, and criminality, but also their awareness about the illegality of their actions. Indeed, one officer mentioned a cybercriminal trader he investigated exchanged emails with suppliers mentioning his criminal trial in another region following previous illegal trades, therefore acting in favour of the prosecution as he showed awareness of the criminal nature of his acts (P-W2). Such resources can stem from several entities, including other Police agencies and private organisations.

Different Police forces have been exchanging information and expertise worldwide. The Police being a vast entity, some agencies have been created to provide information, resources, and expertise to others. This is the case for international organisations building capability in countries whose legislations and procedures are not yet up to par (P-W1, P-W3). This has so far included building facilities such as forensic labs for electronic data analysis (P-W3), establishing Internet-dedicated crime units (P-W1), and providing training and mentoring on best practices (P-W1, P-W2, P-W3), for instance. Specialised units focussing on drug and wildlife trades often support local forces on their most complex cases, as they have more knowledge and expertise, and can advise on the best procedures to follow for warrants and prosecutions, as well as performing these duties alongside the relevant forces (P-W2). However, even these specialised units need to receive expertise from forensic experts to identify a drug or species and attest to the seriousness of this crime in court (P-W2).

Exchanging information about strategy, expertise, or even criminals' personal characteristics is normal practice (P-D2). But it is important to note that when sharing information with foreign forces and companies, the Police, and others, need to abide by their data protection and privacy rules (P-D2, P-W2, P-W3), including GDPR, new Data Protection Regulations in Europe. It was therefore posited that a third party might be best placed to gather all information and feed it to different entities, acting as a conduit for a large audience in this case (P-D2). This has been attempted by several umbrella organisations as they gather and disseminate guides and best practices (P-W1), as well as facilitating communication and exchanges between agencies (P-W1).

While the Police admit to not being able to work with private organisations on a deep level, they agree their intelligence and expertise is complementary and invaluable to their activities and there is a real need for both entities to tackle this problem together (P-D2). Many NGOs and individuals have therefore been passing information on (P-W2) to help enforcement (P-D3).

> *[Do you monitor these platforms?] "No, not really. There are lots of people monitoring them because they are interested in doing so, they tell us and we will then pass that intelligence on to the different police forces." (P-W2)*

Despite their central role in policing, the Police are therefore no longer alone in the disruption of cybercrime, but they benefit from the intelligence and expertise provided to them by experts in drugs, wildlife, and online trade. By outsourcing this initial step in the policing process, although it is often believed to be the sole remit of the Police due to the sensitive nature of the content that might be uncovered (Delpeuch and Ross, 2016), the Police are acknowledging that this process can be performed more efficiently by others (Hutchings et al., 2016), as the need for information sharing and intelligence capabilities increased (Lewandowski et al., 2017). They can therefore focus their efforts where their own strengths and powers lie. Indeed, once information and expertise are shared with them, the Police's investigative work can truly begin.

4.2.2 Information gathering

Police interviewees talked about how important data on Darknet markets and other web and social media sites was, allowing them to obtain information about individuals of interest (P-D1, P-D2, P-D3, P-W2, P-W3). However, there is only so much information private organisations, big and small, can provide the Police with (P-W2). It is therefore up to Police agencies themselves to perform follow-up investigations and to dig deeper into the platforms, content, and cybercriminal traders brought forward (P-W2, P-D3). The Police are able to officially request information from legal platform administrators as part of their investigations, including additional data about specific sellers, the listings they posted on their site, and any additional personal details they have access to (LP-W1), as long as they abide by national legislations (P-W2). A platform administrator confirmed the Police contacts them for data on an almost daily basis across varying issues (LP-W1).

> *"We then have to do some digging to find out more. So for instance, someone has found this person selling ivory, we can then get in touch and open an enquiry with eBay to find out what else they have sold and if it's the only item they have sold very often we will just tell the local Police and say 'here is for interest, deal with that individual'. But if we find a person that has sold 200 items that's far more up our street, so it's that enhancement that we do because they can't tell us everything. They can tell us everything they know, but we really do need to know a bit more before we actually take things forward." (P-W2)*

While scraping the Internet for relevant information is a task too voluminous for the Police to perform alone, gathering further information on specific platforms, products, or persons of interest can only be performed by the Police given their specific powers and authority. Although the Police cannot task external organisations with investigating specific themes or platforms, it can request further details to these organisations that only they would have access to as part of their work (LP–W1). As such the Police can collaborate with other agencies to ask for information about platforms and people in several jurisdictions, helping them to paint a fuller picture as part of their investigations.

Such information is sought for both drugs and wildlife, as the Police seek to have as much data as possible to warrant intervention and legal action (P-W2). This step is therefore crucial to the identification of relevant criminals and their trades, setting the foundations for targeted and effective interventions.

4.2.3 Operation conducting

In the early 2000s, illegal trade happened on the street and could be interrupted by the Police walking past, but the Internet now allows for fewer chance encounters and is therefore less regulated (P-W2). Nevertheless, the Police have been involved in several digital operations aimed at policing online illegal drug and wildlife trades.

Due to the differences in operations conducted by the Police in both realms, this section is divided between drugs and wildlife findings.

The policing of illegal drug trade, whether online or offline, has been a public phenomenon for decades, so many of the operations conducted to stop this trade should be familiar, including Darknet market takedowns and takeovers, arrests, slander and Sybil operations, and prevention.

The Police have been conducting Darknet market takedowns since 2013 when Silk Road was shut down in the biggest Police Darknet market operation at the time.

> *"So basically Silk Road set the example for law enforcement in order to take [these markets] down. We didn't have to convince everybody that this was a very bad marketplace on the Dark Web, it was clear by then." (P-D2)*

These operations have been the sole remit of the Police, often working in conjunction with other international forces (P-D2), as private organisations can only provide information but not take action in this way (POI–D2). However, takedown operations have been criticised as they often lead to the relocation of trade on other marketplaces. Indeed, by taking down the infrastructure of a market, the Police are only taking out the middleman, but demand and supply are still present and will work to generate another marketplace, which will be harder to monitor (POI-D4) and to eventually take down (POI–D2).

"Law enforcement was somewhat criticised because vendors and buyers move on to another [market] and that one will be even bigger. And that was somehow true because we were taking down services and arresting people or sometimes not, and that meant that they could easily continue business on other markets or markets could pop up in different looks and spheres with the same buyers and vendors." (P-D2)

The Police understand this criticism but still plan to use these operations "*every once in a while*" to show cybercriminal traders that they are still present on these marketplaces and able to perform big operations (P-D2). Additionally, variations of takedown operations have also been performed where information was gathered about cybercriminal traders, to elicit psychological distress (POI–D2).

Two of the biggest marketplaces in 2017, AlphaBay and Hansa, were taken down in a coordinated action in the summer of that year. The operation consisted of Hansa being taken over by the Police in order to witness cybercriminals relocating to the marketplace following AlphaBay's orchestrated demise, an operation called a honeypot. The strategy worked and thousands of AlphaBay users flocked to Hansa. As Hansa was a Dutch marketplace, a Dutch Police officer was responsible for ensuring that all orders placed on the marketplace were actually received, so that users would not suspect Police involvement during the information gathering period (P-D2). This was a novel operation in this context, as Dutch law prevents officers from letting drugs pass into other countries and urges them to intervene (P-D2). Hansa ended up being the Dutch Police's "*most prolific case*" as cybercriminal traders never expected the Police to take over an entire marketplace (P-D2). Indeed, although cybercriminal traders always assumed that the Police might be present on the Darknet and monitoring trading activities, this operation confirmed their suspicions and eroded trust among users, as they no longer knew who was a Police officer and who wasn't (P-D2).

"I think Hansa and AlphaBay, but mostly Hansa, changed that because the goals we set for the investigation were basically first to gain as much information about the top vendors as we could, and to obtain as much Bitcoin as we could to hurt them in their wallets. And I think Hansa was at that time again one of the takedowns that created distrust. One could see that after Hansa was taken down

a lot of the regular big vendors did not appear under their own nickname and the use of hidden services was down." (P-D2)

The information gathered during the takeover then allowed the Police in the Netherlands and elsewhere to identify and arrest several cybercriminal traders (P-D2).

While some approve of arrests and their potential impact on other users perceiving higher risks of detection (POI–D4), others expressed concerns that arrests were not the best ways to disrupt these marketplaces: "*the current [arrest] approach is not necessarily the best one*" (POI–D2), "*we cannot arrest ourselves out of this problem of cybercrime, it ain't gonna happen*" (P-D3). One private actor therefore recommended using different arrest tactics to create paranoia on these marketplaces, such as arresting the five most popular cybercriminal traders in one wave and then moving on to the following five most popular in a second wave. This one-two punch intervention would use psychological impact to disrupt trade (POI–D2). Psychological disruption can also be achieved by undermining trust between traders in the way of slander and Sybil interventions.

It has been argued that in certain cases the most effective decision is not to take markets down, as these services could simply relocate, and not to arrest cybercriminal traders, as new traders could come forward, but instead to obtain information and undermine these traders (P-D1, P-D2). Darknet markets are hosted on an anonymous and encrypted part of the Internet, allowing cybercriminals not to be reliant on trust when it comes to their anonymity and privacy while conducting criminal activities online (P-D2). However, the trading component of these marketplaces means that users need to put some trust into other cybercriminal traders for the market to succeed (P-D2). For this reason, participants in industry speak highly of slander and Sybil operations, as trust is more difficult to rebuild than infrastructure after it is damaged (POI–D2). Exit scams performed by market vendors and administrators have also helped this strategy, as "*people themselves have become less trusting and that just erodes communication*"; these operations can therefore build on that premise (POI–D2). Operations like slander and Sybil will make it harder for people to trust one another, and it is expected this mistrust will drive prices up to ensure the right escrow services and cybercriminal trader validations are put in place (POI–D2). The Police and others will need to follow where this trade might relocate to if these mechanisms are not successful and trust

becomes impossible to rebuild on Darknet markets (P-D2). However, these operations are highly regulated as certain legislations prevent Police officers from enticing others to buy illegal products (P-D2), so they cannot be conducted everywhere. A private organisation also spoke about experimenting which such tactics following ethical approval from their leadership in order to witness trends in trading volumes after such interventions (POI–W6).

As well as reactive operations when Darknet markets have already formed, the Police have engaged in prevention, catching cybercriminals at the beginning of their criminal careers as opposed to waiting and taking more drastic action further down the line (P-D3). The UK prevention programme is based on what arrested cybercriminals said would have been helpful along their criminal paths (P-D3). These operations often consist of cease-and-desist interventions, sending officers to individuals' houses, making them aware that the Police know of their illegal activities and offering them an opportunity to stop by signing a document (P-D3). After they have been made aware of the law and committed to stopping, further offenses aggravate their case (P-D3). This prevention strategy has been a significant part of the British national security approach to cybercrime and it is being rolled out internationally following the UK's success (P-D3). These operations have been shown to work particularly well on less informed individuals. Indeed, when the Prevent team first started its cease-and-desists in 2012; a criminal group they targeted was surprised they were not arrested, likely because the Police had only witnessed a small part of their illegal trading activity (P-D3). This group might have therefore been too far along by the time they were identified and approached. Collaboration is consequently paramount for the Police to gather a full picture of these cybercriminals.

Other strategies have been at the forefront of online illegal wildlife trade policing, including seizures and the suggestion of content to be blocked and users to be removed by legal platform administrators.

Most illegal wildlife trade happening online is "*pretty obviously illegal and not well hidden*" (P-W1), showing that crackdowns on this type of trade are not yet stringent enough to force criminals to find a more complicated and discreet way to trade (P-W1) and that the Police and platform administrators need to be more proactive on cracking down on websites and listings. Indeed, the policing of illegal wildlife trade online is still in its infancy as it has been overtaken by the policing of other more dangerous and urgent types of crimes. Additionally, Police units are often small and lacking resources, meaning they need to focus on large and valuable cases (P-W2).

> "*Wildlife crimes are generally quite low down in the list of priorities when you think about the other things the Police have to investigate" (POI–W4)*
>
> *"There is a question of priority if you look at how bad the problem of child sexual exploitation is online" (POI-W3)*
>
> *"It will never be [a priority], at the end of the day someone has had their child stolen versus someone shot a tiger, that's just how it is and it will always be that way" (POI–W2)*
>
> *"Irrespective of how they feel about wildlife, they are outstretched and under-resourced" (POI-W3)*

Seizures have been conducted when the Police have come across prolific vendors, likely to hide large volumes of valuable products and specimens. When online illegal wildlife trade policing began in the UK in the mid-2000s, the Police took an interest in rare vendors posting only a few listings online and sometimes discovered much larger stocks than expected upon seizures (P-W2).

"Somebody was advertising skulls on eBay […] so when we actually went to do the warrant, we found there were about 5 or 6 items advertised [online] at any one time so we were expecting to find a handful of items, but when we got there it was absolutely full of skulls and various other things, including a package that had literally just arrived from South Africa with dried skins and taxidermy items in it, mislabelled, that had just gone through the post, and also quite a lot of things that had come through the supplier in Java. […] The superficial image that we had before we went in was actually nothing like what was going on in reality, the scale was a lot bigger because it had gone below the surface with people that they trusted at that point." (P-W2)

Since then, the number of seizures for wildlife products have greatly increased and happen frequently in various countries around the world (POI-W3).

"There are more seizures, there is greater awareness, it's become part of law enforcement officers' mandate and responsibility, and that is now widely understood at most border crossings in most countries of the world that wildlife crime and wildlife trade is a thing […] 20 years ago we wouldn't even think to look" (POI-W3)

While seizures were not mentioned by interviewees talking about drug trade, news articles and reports in the following section show this operation is also paramount to the policing of online illegal drug trade.

Although the Police have no power or authority to remove illegal content or block users on legal platforms, they can inform platform administrators and moderators about illegal listings and incite them to do so (P-W2).

[Can you ask platforms to take an advert down or to block a seller?] "No, all we can do is tell them what we know […], if somebody is regularly trading, we can say 'this person has committed offenses', and it is up to them to decide to give them a warning or ban them." (P-W2)

The final decision therefore remains with the legal platforms based on their policies, national regulations, and the extent of the listings' illegality, as certain products or photos are more difficult to assess than others. Indeed, some wildlife listings for example are explicitly illegal when they do not involve trading certificates (P-W1), though others might include falsified ones (POI-W1).

Given their powers of search and arrest, the Police are the only group in the online illegal drug and wildlife trades policing network that can perform policing operations, with the exception of legal online platform administrators and moderators who are responsible for removing criminal users and content on their own sites, as discussed in the next chapter. These operations have taken several forms over the years, although those differ between online illegal drug and wildlife trades, after the first two common activities. Indeed, the policing of online illegal drug trade currently relies on the takedown of marketplaces' infrastructure, and the arrest of traders and administrators. More preventative work rather than just reactive has also been taking place, trying to dissuade people from taking part in such behaviours. Recently more covert interventions have been employed to disrupt trust on Darknet markets, as this is believed to spark longer-term results than the disruption of networks and infrastructure. This type of operation is explored further in the final chapter of this thesis.

The policing of online illegal wildlife trade, however, is mainly focussed on seizing products in their transit, and working alongside platform administrators and moderators to remove illegal content and block users taking part in criminal activity on their sites. These seizures have also been argued to be mostly incidental, as the Police often intercept wildlife while investigating 'more serious' criminal matters (Runhovde, 2017). However, it should be noted these interventions often focus on live animals and animal products rather than plants (Margulies et al., 2019; Lavorgna and Sajeva, 2020) This more limited involvement of the Police in the case of illegal wildlife trade reflects their lack of resources and ability to police wildlife crime, specifically given their lack of access to legal online platforms and knowledge about wildlife, as opposed to drugs. This gap in intervention, or its much smaller volume compared to drug interventions, has therefore been filled by other actors, not only including NGOs (Nurse, 2013) which have taken the lead on the policing of an important crime in the eyes of the public (Button, 2019), but also by legal platform administrators and moderators who are responsible

for the legality of activities on their platforms. Both of these actors and the collaborations between these groups are explored in later chapters.

The final activity for both types of trades is for the Police to report on their and others' interventions.

4.2.4 Reporting

Following the conduct of various operations on their own, with other Police forces, or with the support of legal platforms and private organisations, the Police then report on their actions, not only as a way to pursue legal action, but also to raise awareness about these trades.

The ultimate goal of the Police following the gathering of evidence and conduct of operations is to bring criminals, cybercriminal traders or otherwise, to justice, ideally in their own country (P-W2). The more data they are able to collate from private organisations and platform administrators the more evidence they will be able to present in court to show criminal intent and wrong-doing to justify a large sentence (P-W2). Beyond informing the courts, the Police also inform the public about these wrong-doings.

Awareness raising falls under the remit of larger Police organisations, which have the capacity to speak regularly, write longer thematic reports about their activities in specific areas or collate external knowledge about the topic (P-W2, P-W3). Due to their subject-matter expertise and on the ground experience, officers are also often invited to open forums to provide feedback about the practicalities of new legislations and to spark changes if the language or content are not accurate (P-W2). Although this activity is very limited, some interviewees even spoke about giving lectures and talks at universities to students enrolled in Law or related programmes to educate them about their work (P-W2).

Although reporting is not every Police agency's main purpose (P-W1, P-W3), it is important for them to write documents of different formats to inform the public about their and others' policing actions, even if it sometimes takes months for criminals to go through trial and conviction and for cases to be officially closed (P-W2). Some agencies are so small and specialised that they depend on others to communicate their impact for them, which

sometimes leads to them not being acknowledged in public operational reports (P-W2). Other agencies admitted to not having set communication frameworks for their presence on social media for instance (P-W3). Communications can therefore vary widely between teams based on the preferred practices of their leaders (P-W3). In any case, it was agreed that Police agencies should proudly and publicly report on their activities, as well as commending those of others in the field (P-W2, P-W3).

Due to the differences in operations performed and the ways reporting organisations mentioned them, this final section is also divided between drugs and wildlife findings following the content analysis of online illegal trade related documents.

Throughout the 90 analysed Police online illegal drug trade related documents, 739 references were made to 13 different policing operations. Market takedowns were the operations referenced the most with 188 mentions, closely followed by 175 mentions of seizures, whereas scams and the law were the ones referenced the least with only two mentions each. The other nine operations were mentioned between eight and 137 times. It should be noted that slander and Sybil operations were not mentioned in any of the analysed publications. However, one interviewee confirmed these interventions were taking place to a degree that could not be disclosed (P-D2). A graph is presented below of all the online illegal drug trade operations referenced in these documents and the nature of their mentions.

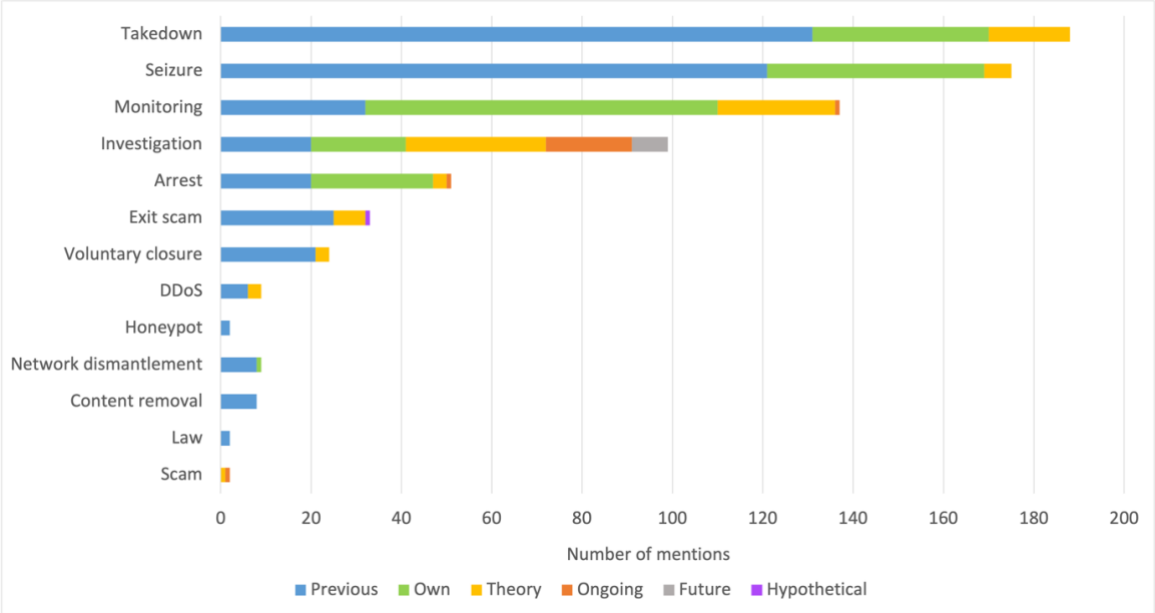


Figure 4.1: Overall number and types of mentions of different online illegal drug trade policing operations

While gathering which types of operations are mentioned in these documents is important to understand what the Police talk about in their communications, this chapter focusses on the *ways* these operations are mentioned. Further details of the six different types of references mentioned in the Police's public communications about online illegal drug trade policing are provided below.

With 396 mentions, or just under 54% of total references, previous operations were the ones mentioned the most across documents.

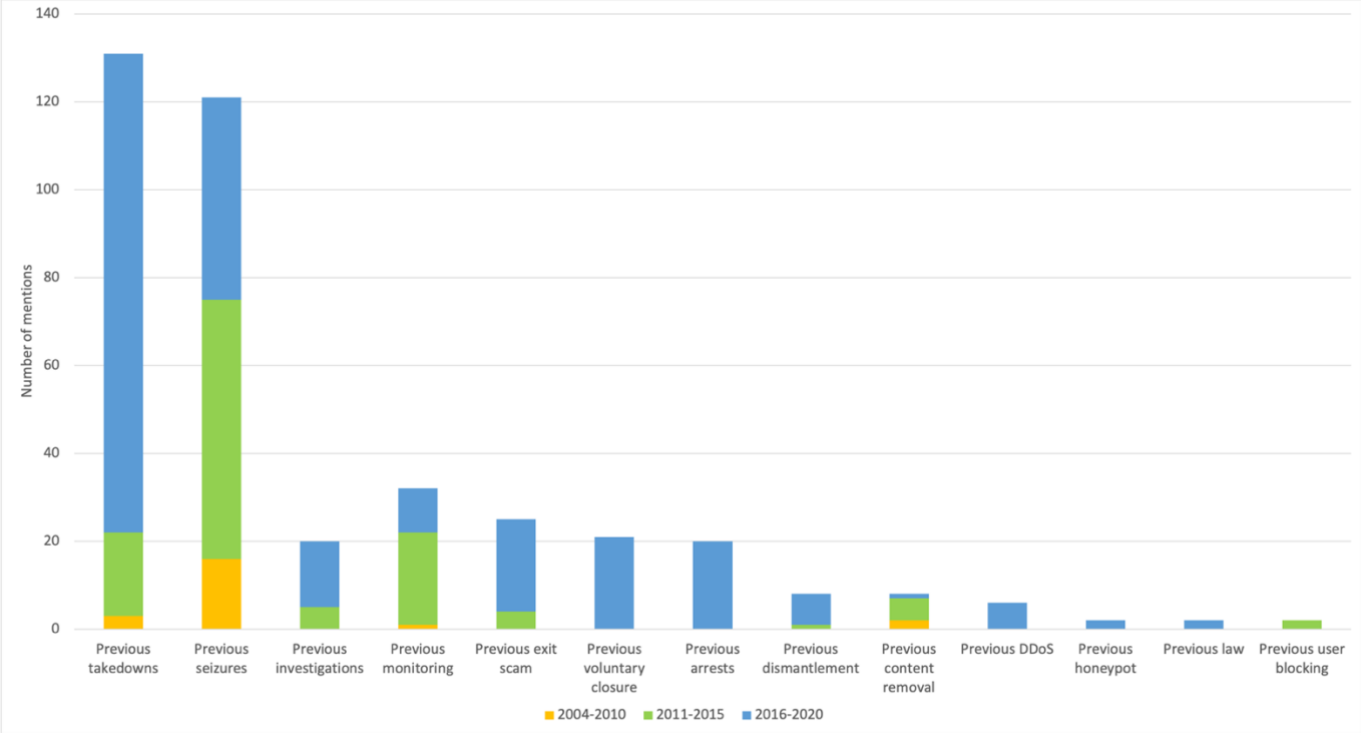


Figure 4.2: Overall number of mentions of different previous online illegal drug trade policing operations over time

Previous operations are ones that were conducted in the past but that reporting agencies did not have a direct involvement in (or if they did, they did not explicitly report it). These previous interventions take the form of direct operations against criminals and trade, background work in order to perform these direct interventions effectively, and disruptive activities performed by others in the ecosystem.

Previous takedowns were referenced the most in this category, as many examples of illicit websites but also Darknet markets such as Silk Road, AlphaBay, Hansa, RAMP, xDedic, and others shaped the online illegal trade ecosystem over the last decade. These references mentioned varying levels of details about what the markets were, who was involved, the volume and value of trade they engendered, and where their servers were located (EMCDDA & Europol, 2011, 2013a, 2014g, 2016b, 2017a, 2019; Eurojust & Europol, 2019; Europol, 2015c, 2016b, 2017f, 2018c, 2019b, 2019f, 2019g, 2020e; UNODC, 2014, 2016a, 2017b,

2018b, 2018c, 2018d, 2018e, 2018f, 2019a, 2019b, 2020c, 2020d; WCO, 2009a, 2010a, 2010b, 2011, 2012c, 2013a, 2013c, 2014b, 2015b, 2016d, 2018). In the case of Hansa, the running of the marketplace as a honeypot in order to gather information about users following the closure of AlphaBay was also referenced (UNODC, 2019a, 2019b). Seizures were also mentioned several times, as they convey the amount of work and collaboration performed by various agencies in order to intercept goods of diverse shapes, forms, values, and volumes during their transit (EMCDDA & Europol, 2007, 2012a, 2012b, 2013a, 2013c, 2014b, 2014c, 2014f, 2014g, 2015b, 2016c, 2016d, 2017a, 2017b, 2017c, 2019; Europol, 2010b, 2019b, 2019f, 2020d, 2020f; UNODC, 2014, 2015, 2017d, 2018c, 2019a, 2019d, 2020e; WCO, 2014a, 2015d, 2016d, 2020a). Another direct intervention, although it is mentioned less, is arrests, with a few publications mentioning administrators and vendors had been arrested following their criminal activities, many being named and geolocated (EMCDDA & Europol, 2017a, 2019; Europol, 2018c, 2019b, 2019f, 2020d, 2020f; UNODC, 2019b, 2020d; WCO, 2020a). When several arrests took place simultaneously or a network was significantly impacted by human or structural interventions, reports spoke of 'dismantlement', including the number of people affected and where their networks were active (EMCDDA & Europol, 2017a, 2019; UNODC, 2019d, 2020d; WCO, 2014b). Agencies sometimes also spoke about removing illegal content online, either taking down webpages on their own if these sites were illegitimate or with legal platform administrators if they weren't (WCO, 2009a, 2010b, 2012c, 2013a, 2013c, 2014b, 2015b, 2020a).

Documents also often reported on previous monitoring and investigations performed to reach takedown and seizure stages. The difference between monitoring and investigations here is that the former is more passive, monitoring several people and marketplaces to witness whether any criminal activity is taking place, and only leading to investigation if pertinent information comes to light. However, the latter is more active, as the Police already have a lead into a specific person or site and are looking for further information. In both cases, agencies spoke about the investigations others took part in in order to apprehend a specific criminal or shut down a market (EMCDDA & Europol, 2014f, 2014g, 2017a, 2019; Europol, 2019b, 2019f), as well as the constant monitoring they were involved in to gauge activity on several marketplaces and have specifics to investigate later on (EMCDDA & Europol, 2011, 2012a, 2013c, 2014d, 2014g, 2015b, 2016a, 2016b, 2019; Europol, 2010a 2015c; UNODC,

2018c). These two interventions were mostly mentioned by EMCDDA and Europol in their common publications, as they reported on new drugs traded online and any information and trends of interest. A couple of documents even mentioned the writing and implementation of laws against online illegal trade in order to act more preventatively (UNODC, 2017d, 2020e).

Despite exit scams and voluntary closures not being performed by Police agencies, they were also included in these documents as disruptive interventions. Several exit scams were pointed to in the past five years, often including the markets' names, the length of time they had been operational, and the amount of users they left out of pocket (EMCDDA & Europol, 2017a; Europol, 2015c, 2016b, 2018c, 2019f, 2020e; UNODC, 2017b, 2018c, 2019b, 2020c, 2020e). Similarly, several marketplaces were named as having voluntarily closed during the same period, adding to fluctuations in the ecosystem and showing to readers that trading on Darknet markets is not necessarily a safe bet (EMCDDA & Europol, 2017a; Europol, 2016b, 2018c, 2019f, 2020e; UNODC, 2016a, 2018c, 2019a, 2019b, 2020e). These closures were sometimes impacted by Distributed Denial of Service attacks potentially performed by competitors and which seem to have become more common recently (EMCDDA & Europol, 2017a; Europol, 2019f, 2019g, 2020e; UNODC, 2018c).

With 214 mentions, or just under 29%, own operations are the second most used reference type, relating to operations agencies directly took part in on their own or alongside others.

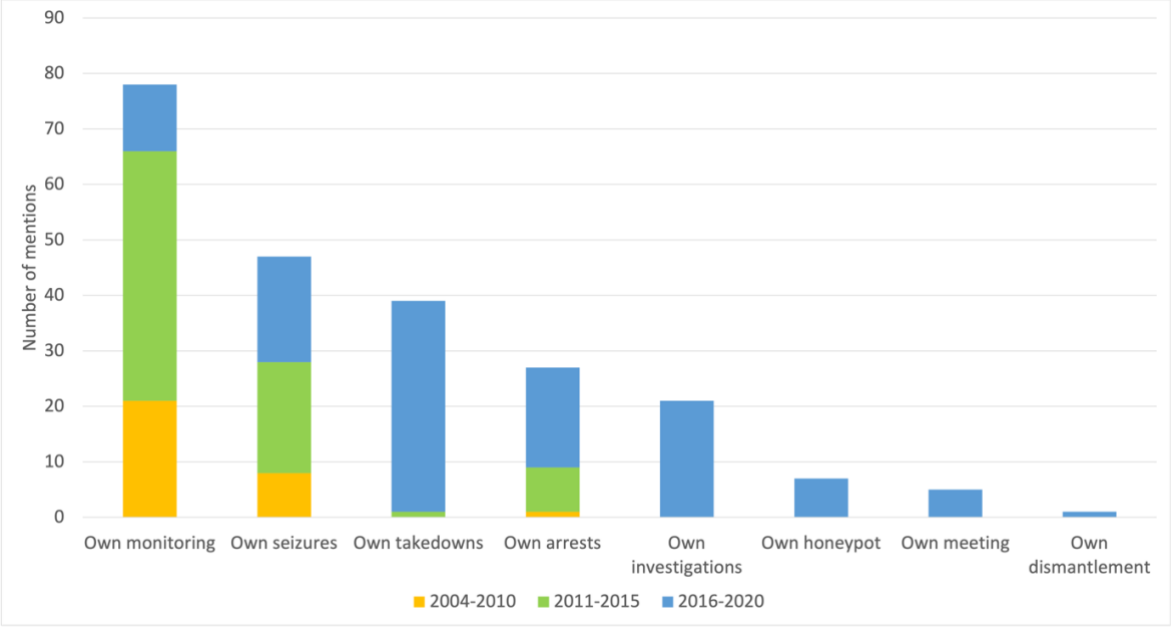


Figure 4.3: Overall number of mentions of different own online illegal drug trade policing operations over time

As well as the previous operations mentioned above, many agencies reported their direct involvement in policing interventions, whether direct or preparatory.

Direct interventions conducted by reporting agencies included seizures, in large numbers by the WCO as parcels are intercepted when crossing borders, but also by Europol providing support to and coordinating activities between national Police forces. These recent drug seizures included details about the volumes that were intercepted, where, and the shipments' provenance (EMCDDA & Europol, 2017a, 2019; Europol, 2017a, 2017f, 2019c, 2019d, 2019e; WCO, 2009a, 2010a, 2010b, 2011, 2012a, 2012c, 2013a, 2013c, 2014b, 2015b, 2016d, 2018, 2020a). Agencies also reported on takedowns they were involved in, namely Operation Onymous, which involved the simultaneous closure of hundreds of marketplaces, and the shutdown of AlphaBay (EMCDDA & Europol, 2017a; Europol, 2015c, 2017a, 2017e, 2018a, 2018c, 2019a, 2019b, 2019c, 2019d, 2019h, 2020d, 2020e), which was also coupled with the running of Hansa as a honeypot by the same agencies (Europol, 2017e, 2017f, 2018c, 2019b, 2019c). Following both seizures and takedowns, several reports mentioned the arrest of administrators or traders, following their intelligence or through their own agents (EMCDDA

& Europol, 2017a, 2019; Europol, 2017a, 2017e, 2017f, 2017g, 2019a, 2019b, 2019c, 2019d, 2020e; WCO, 2010a, 2011, 2012a, 2012c, 2013a, 2013c, 2015b, 2016d, 2018), as well as the dismantlement of wider networks when several criminals were apprehended at the same time (Europol, 2020f).

Beyond direct interventions, reporting agencies were also transparent about the indirect and behind-the-scenes work they performed, from monitoring marketplaces, drugs, and people (EMCDDA & Europol, 2008, 2009, 2011, 2012a, 2012b, 2013a, 2013c, 2014b, 2014c, 2014e, 2014f, 2014g, 2015a, 2015b, 2016b, 2016c, 2016d, 2017a, 2017b, 2017c, 2019; Europol, 2010a, 2010b, 2014a, 2014b, 2014d, 2016a, 2017c, 2019d), to investigating criminals and sites more specifically (EMCDDA & Europol, 2017a; Eurojust & Europol, 2019; Europol, 2017a, 2018a, 2018c, 2019a, 2019e, 2020e; WCO, 2018).

There were 98 references to operational theory, just over 13% of total mentions.

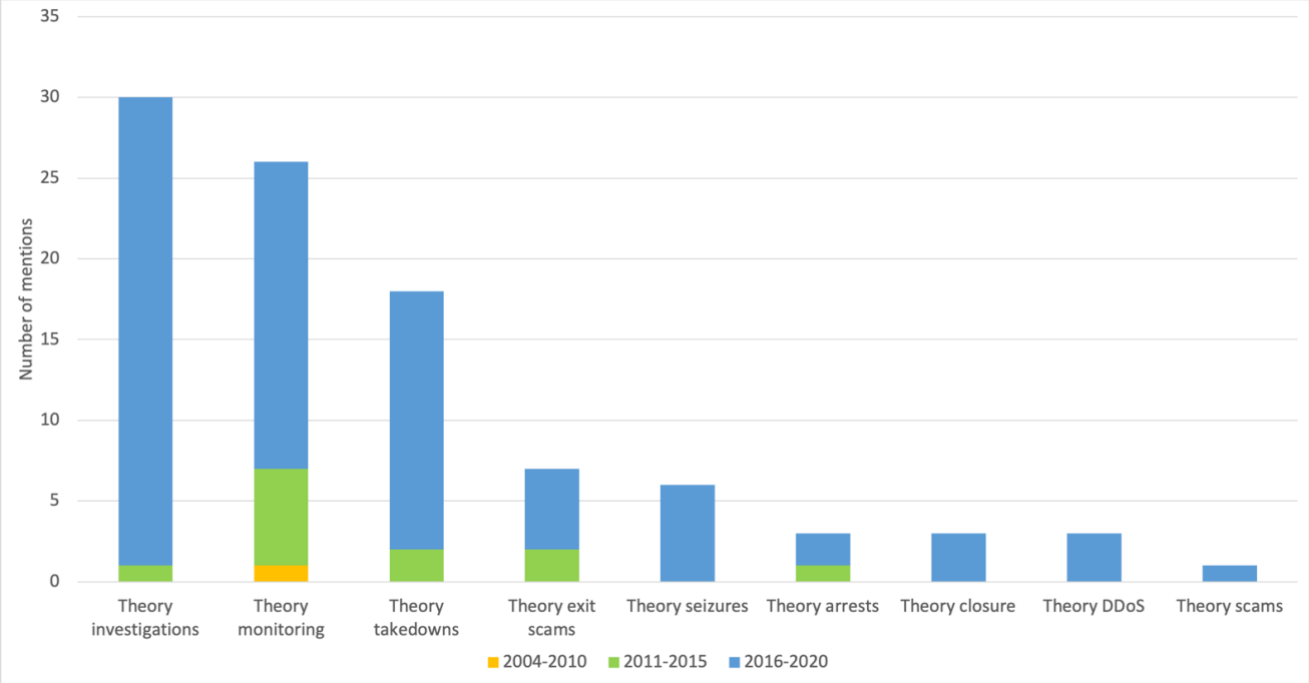


Figure 4.4: Overall number of mentions of different online illegal drug trade policing operation theory over time

As well as factually reporting on previous operations they or others played a part in, agencies involved in this analysis also spoke more theoretically on several occasions. There were two kinds of theoretical references, depending on the intervention under scrutiny: an explanation about why specific interventions are prescribed and the benefits they bring, and an analysis in broad terms about the consequences of certain intervention types.

Most of the references in this category related to marketplace monitoring. This was closely followed by investigations, as agencies throughout the years argued that monitoring was a beneficial activity to conduct on both surface and Dark markets, following the development of the necessary web-based tools to that effect. This monitoring would not only provide them with a better understanding of the scale and scope of this trade, but it would also yield closer interactions with other agencies also involved in this process (EMCDDA & Europol, 2012b, 2013b, 2017a, 2019; Eurojust & Europol, 2019; Europol, 2010a, 2014c, 2015c, 2017b; UNODC, 2020c). They also argued resources should consistently be put into investigations in order to apprehend criminals and stop this trade effectively (EMCDDA & Europol, 2013b, 2017a, 2019; Europol, 2018b, 2019d, 2019f; UNODC, 2012b; 2017a). Seizures were advocated for in a similar manner, as traders are exploiting postal and delivery systems already pushed to their limits by the general rise of online orders, and this can allow for the tracking of individuals and products for future interventions (EMCDDA & Europol, 2017a; Europol, 2019d).

Additional mentions referred to direct interventions, their logistics, and their consequences. Takedowns were a prime example of this theoretical perspective, as several publications mentioned takedowns were initially effective but then led to new marketplaces forming. A specific trend showed new marketplaces were likely to be small and decentralised, so as not to attract Police attention, showing the resilience of the ecosystem (EMCDDA & Europol, 2017a, 2019; Eurojust & Europol, 2019; Europol, 2014c, 2017e, 2019f, 2020d, 2020e; UNODC, 2019b; WCO, 2012d). The arrest of cybercriminal traders was also argued to lead to other network nodes replacing them and taking over criminal activities (EMCDDA & Europol, 2017a; Europol, 2014c; 2020d). Other documents explained what exit scams consisted of, and the potential distrust they instilled in the Darknet market ecosystem following previous exits recently witnessed (EMCDDA & Europol, 2016b, 2017a, 2019; Europol, 2015c, 2017e; UNODC, 2020e). Voluntary closures by administrators were also touched upon, as they might show a

fear of Police closures (EMCDDA & Europol, 2016b, 2019; Europol, 2017e), but also act as responses to other interventions such as Distributed Denial of Service attacks (EMCDDA & Europol, 2016b; Europol, 2019g). Finally, scams performed by vendors on these marketplaces were briefly mentioned, as they theoretically disrupt trust (EMCDDA & Europol, 2019).

There were 22 references to ongoing operations, just under 3% of the total mentions.

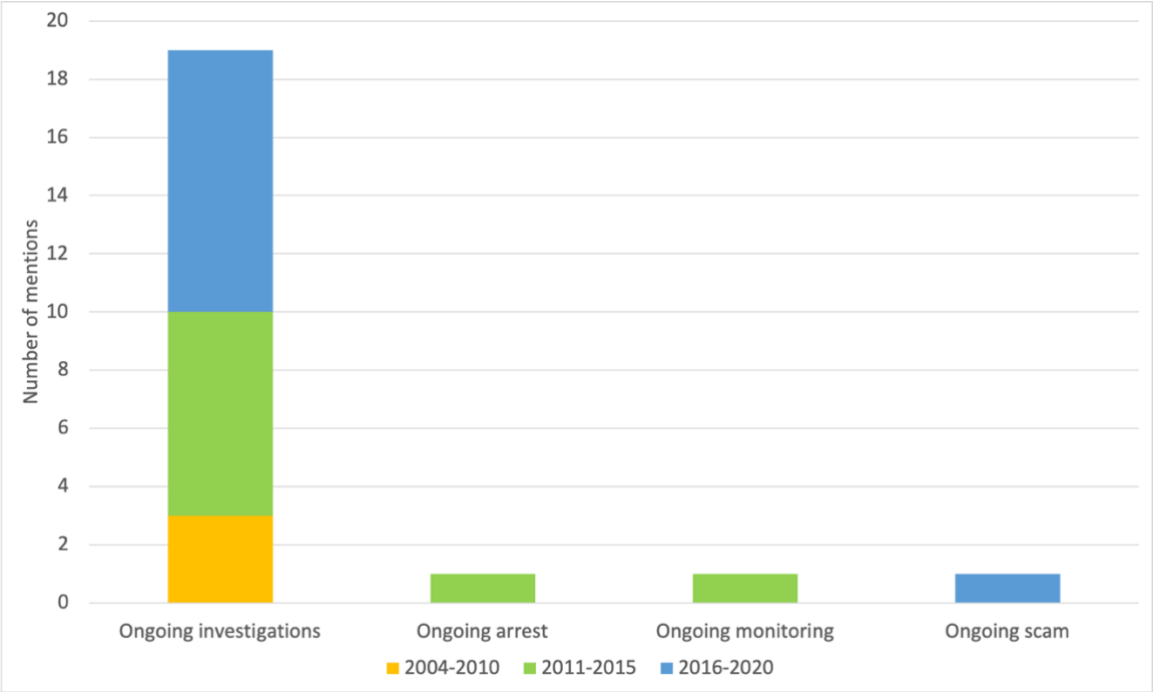


Figure 4.5: Overall number of mentions of different ongoing online illegal drug trade policing operations over time

Throughout the reporting period, a few publications mentioned policing interventions that were ongoing, although very few compared to past interventions. As this is likely the least revealing, ongoing investigations were the operation type referenced the most in this category, and several agencies admitted to currently looking into various unnamed marketplaces and criminals (EMCDDA & Europol, 2017a, 2019; Europol, 2019d, 2020d; WCO, 2009a, 2010a, 2010b, 2011, 2012c, 2013c, 2014b, 2015b, 2016d). Similarly, one reference was made to an ongoing marketplace monitoring (EMCDDA & Europol, 2012b). One report also documented the ongoing arrest of a cybercriminal trader (WCO, 2011), but this type of reference has not re-occurred in more recent years. Fewer details were also given in this case than would have been shared if operations had already been successfully conducted. Finally,

a recent World Drug Report explained that scams were ongoing on Darknet markets and vendors were fooling buyers into buying products they would not receive (UNODC, 2019b). Although it is also the sole reference of this kind here, ongoing scams have also been recently mentioned in private organisations' drug-related documents in light of challenges brought by the COVID-19 pandemic, as will be discussed in a later chapter.

There were eight references to future investigations to be performed, just over 1% of the total mentions. In recent reports, several agencies started to refer to investigations which would be conducted in the future, following past or current interventions. Several documents therefore mentioned plans to perform additional investigations about specific drugs, people, and sites (EMCDDA & Europol, 2017a; Eurojust & Europol, 2019; Europol, 2018a, 2019b, 2019d, 2019f).

Finally, there was one reference to a hypothetical operation. As shown by the five previous ways operations have been mentioned in the Police's news articles and reports, their content is very factual and evidenced, so hypothetical operations are not expected as part of their communications. However, on one occasion, the Police referred to the administrator of a Darknet market potentially exit scamming its users, closing down the marketplace and leaving with the money held in escrow (EMCDDA & Europol, 2019). As this operation was performed by cybercriminal traders, the Police were not in a position to confirm these facts and only hypothetically mentioned such an intervention was likely to have happened, as the signs in the ecosystem pointed to an exit scam.

The policing operations, the nature of their mentions, and their numbers vastly differ in the context of online illegal wildlife trade, as shown in the next section.

Throughout the 10 analysed Police online illegal wildlife trade related documents, 54 references were made to five different policing operations. Monitoring was the operation referenced the most with 22 mentions and network dismantlement the one mentioned the least with only two mentions. The other three operations were mentioned between four and 17 times. Overall, wildlife-related documents represented only 10% of the total online illegal trade documents reviewed for this study. They also did not reflect the same trends or include the same operation types as drug-related publications. A graph is presented below of all the online illegal wildlife trade operations referenced in these documents and the nature of their mentions.

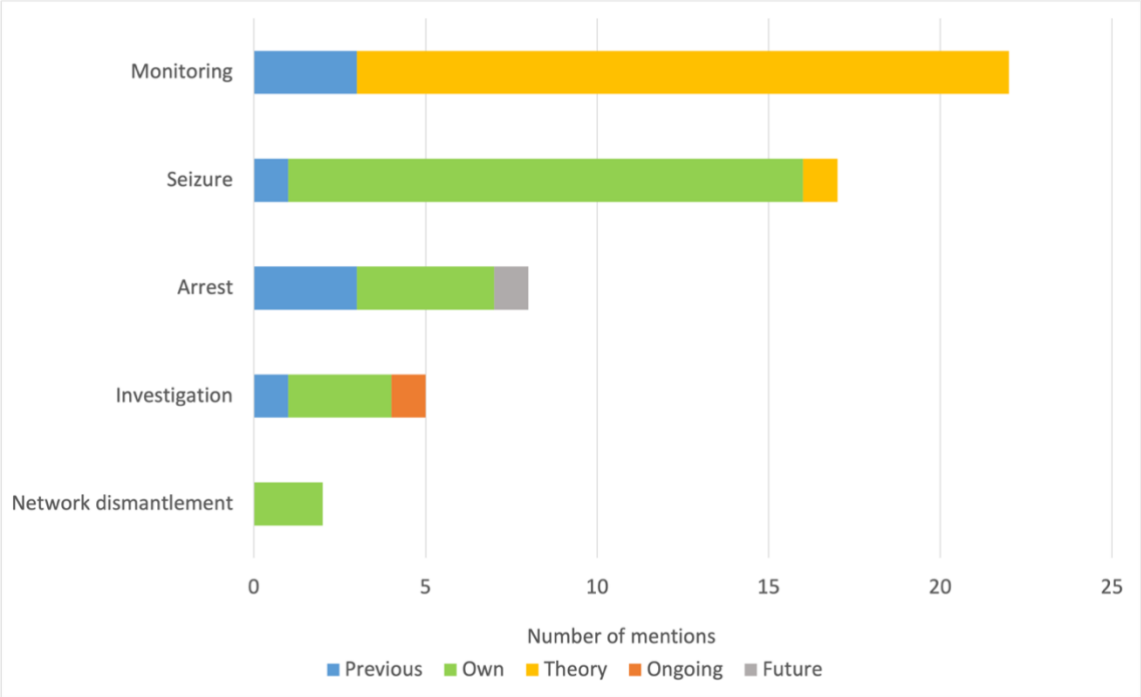


Figure 4.6: Overall number and types of mentions of different online illegal wildlife trade policing operations

Further details of the five different types of references mentioned in the Police's public written communications about online illegal wildlife trade policing are provided below.

With 24 references, or just under 44.5% of total mentions, own operations are the ones referenced to the most across documents, describing operations reporting agencies directly took part in on their own or alongside others.

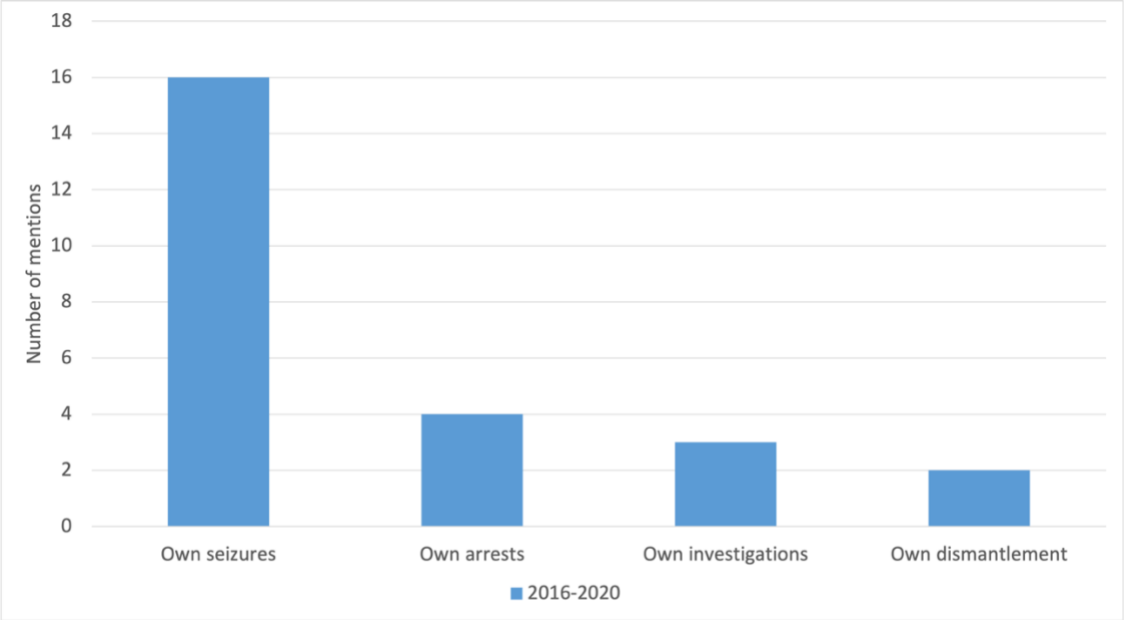


Figure 4.7: Overall number of mentions of different own online illegal wildlife trade policing operations over time

Direct interventions conducted by reporting agencies included seizures, in large numbers by the WCO as parcels are intercepted when crossing borders, but also by Europol providing support to and coordinating activities between national Police forces. Recent seizures included details about the volumes that were intercepted, where, and the shipments' provenance (Europol, 2020a; WCO, 2019b). Several reports also mentioned the arrest of administrators or traders, following their intelligence or through their own agents (Europol, 2020a; WCO, 2019b), as well as the dismantlement of wider networks when several criminals were apprehended at the same time (Europol, 2020a, WCO, 2019b).

Beyond direct interventions, reporting agencies were also transparent about the indirect and behind-the-scenes work they performed, including investigating specific criminals and marketplaces (Europol, 2020a, 2020e; WCO, 2019b).

There were 20 references to operational theory, just over 37% of the total mentions.

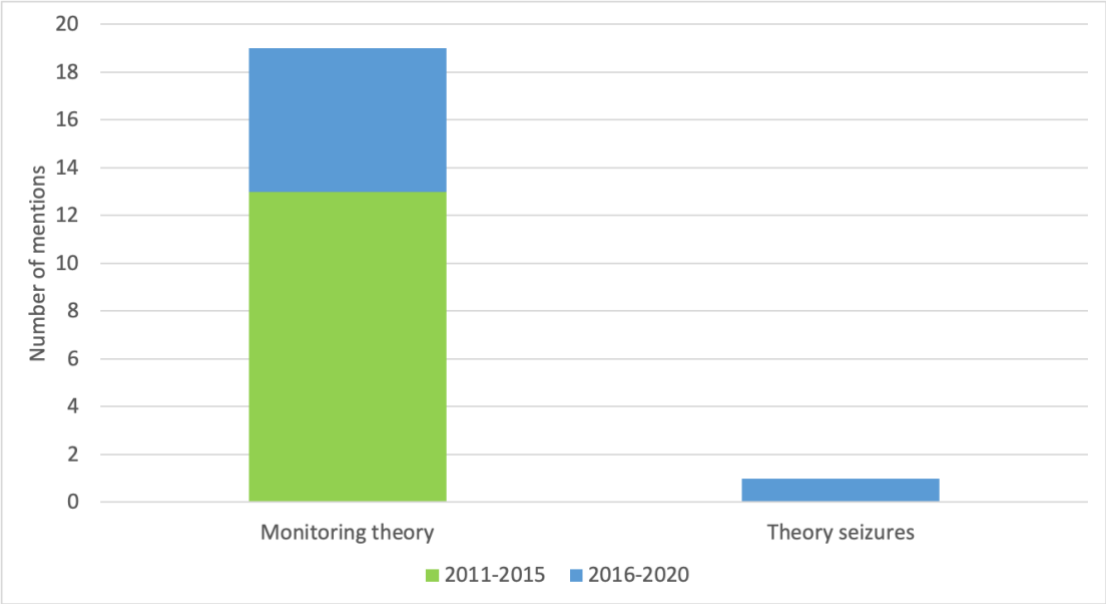


Figure 4.8: Overall number of mentions of different online illegal wildlife trade policing operation theory over time

Agencies throughout the years argued monitoring was a beneficial activity to conduct on both surface and Dark markets following the development of the necessary web-based tools to that effect. Such monitoring would provide agencies with a better understanding of the scale and scope of this trade and lead to closer interactions with other agencies also involved in this process (Europol, 2011c, 2015a; UNODC, 2012a, 2018a, 2020e). Seizures were advocated for in a similar manner, as traders are exploiting postal and delivery systems already pushed to their limits by the general rise of online orders, and this can allow for the tracking of individuals and products for future interventions (WCO, 2019b).

With eight mentions, or just under 15% of total references, previous operations were the third most used reference type.

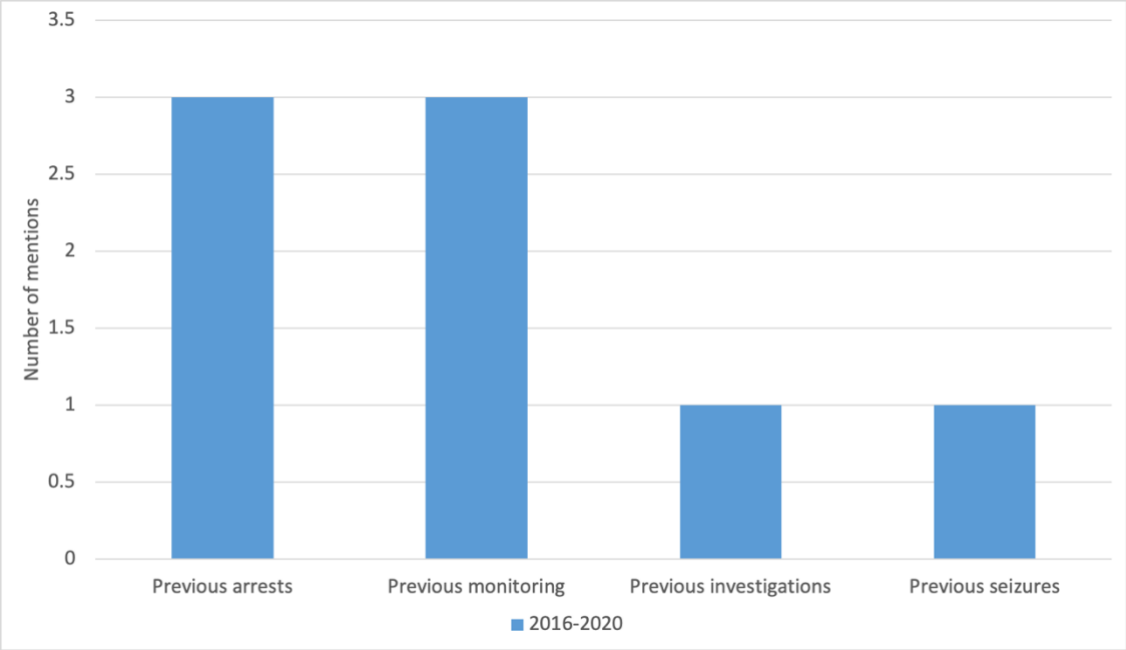


Figure 4.9: Overall number of mentions of different previous online illegal wildlife trade policing operations over time

In terms of direct operations, one publication mentioned administrators and vendors had been arrested following their criminal activities, many being named and geolocated (WCO, 2019b), while another described the seizure of wildlife products (WCO, 2016a). In more indirect terms, publications reported on the investigations others took part in to apprehend a specific criminal or shut down a marketplace (WCO, 2019b). Agencies also reported on the constant monitoring they were involved in to gauge activity on several marketplaces and have specifics to investigate later on (UNODC, 2016b, 2020e).

Throughout the analysed documents, the WCO referenced an ongoing investigation into cybercriminals involved in online illegal wildlife trade (WCO, 2019b).

Finally, the WCO made one reference to a future arrest to be performed following certain criminals' involvement in online illegal wildlife trade (WCO, 2019b).

The final stage of Police intervention in online illegal drug and wildlife trades policing also differed significantly between both products. Indeed, the Police released hundreds of news articles and reports related to drug trade and its policing, 90 of which focused on online policing specifically and are therefore included in this analysis. However, much fewer publications were released about online illegal wildlife trade policing and they were only published more recently. Beyond these numbers, the ways these publications mentioned policing also differed, despite being written by the same agencies. Drug-related publications mostly mentioned previous operations conducted in the drug sphere, some of which they were involved in and some which they explained in more detail in order to justify their use. However, wildlife-related publications mostly referred to operations the reporting agencies were a part of, some of which they justified through theory, and fewer which had been conducted without their support. This disparity reveals the sheer volume of drug-related policing operations, even if they only concern online trade, which the reporting agencies do not always participate in. As fewer agencies are involved in the policing of online illegal wildlife trade, however, their direct involvement was more frequently revealed. In both cases, very few references were made to ongoing or future operations, as these might reveal too much sensitive information, but a few such references were still noted.

Overall, it was important for Police agencies to report on their actions in order to create availability bias for cybercriminal traders, as they come across a large range of content about policing and become more aware that their actions might have consequences (Europol, 2019d), but also to keep their accountability to the public they are protecting (P-W2). Indeed, Police agencies have been formed to protect the public from various harms (Button, 2019). It is therefore important for them to inform this public about the activities they have performed, why they have been undertaking certain activities and not others, and the results they have reached. Knowing cybercriminal traders themselves are part of that public, however, not all operations can be reported on, as more covert slander and Sybil operations require a degree of secrecy. An analysis of the efficacy of these two policing interventions is presented in the last chapter of this thesis.

The answer to our second research question is therefore that the Police perform four main activities when policing online illegal drug and wildlife trades. First the Police receive intelligence and expertise from other policing actors, as they are more numerous and better suited to collect necessary information. The Police then gather further evidence from these leads by investigating cybercriminal traders, marketplaces, and products of interest. Police operations can then be conducted including the takedown of marketplaces, the arrest of traders and administrators, the seizure of products, the undermining of trust through slander and Sybil operations, the suggestion of listings to be removed and traders to be blocked by legal platforms, and the prevention of such crimes. Finally, the Police report on their activities, not only to bring the relevant cybercriminals to justice but also to inform the public they are accountable to, and to signal to cybercriminal traders that they are after them.

Although these broad activities are the same when policing both online illegal drug and wildlife trades, the answer to our third research question is that the specifics of these activities vary at different stages. Indeed, the Police are overall less involved in the policing of online illegal wildlife trade, meaning the direct operations and the reporting they perform are fewer than for online illegal drug trade. All of these Police activities are summarised alongside the activities conducted by legal online platforms, private organisations and individuals, and cybercriminal traders in the policing script devised in the Discussion chapter.

Despite these differences between the policing of online illegal drug and wildlife trades performed by the Police, the ways these policing activities can be rendered more effective in the future are similar for both products.

4.3 The future of the Police

One common theme came from interviewing Police officers and analysing Police agency communications – collaboration. While the academic literature has cited various examples of Police agencies working with one another or with private organisations, these connections are not yet fully formed and remain fragile. Fostering these cross-sector relationships and the trust the Police put into other organisations to support their work will therefore be paramount to increase the efficiency of their interventions.

Interviewees policing both online illegal drug and wildlife trades spoke about the need for multi-disciplinarity and policing in the way of "*coalitions*" (P-D2). Indeed, the Internet is a large ecosystem that involves many stakeholders and "*everyone has their role to play*", from individuals to corporations, to reach this common goal (POI-D1). These groups will ideally involve different points of view, individuals with different skills and expertise, toolsets and ideas that would help solve this problem (POI-D1). Cybercrime in general, and online illegal trade in particular, cannot be disrupted entirely by the Police, government, private industry, non-profits, or academia; they all need to work together (POI-D1, POI-D4).

> *"Everybody needs to understand that there can't be one solution from one government or one organisation, everybody needs to work in this together, and in the end we need to understand that it's not only the criminal justice sector, it goes back to the economy, to culture, to social development, poverty, public health, a lot of other stuff, so we need to understand that obviously society as a whole needs to play a role in this." (P-W3)*

Most interviewees talked about collaboration when describing the direct interventions analysed in the Reporting section, the people they worked with, how, and why. Police operations, such as takedowns and content removals, have involved many forces and organisations over the world collaborating and coordinating their actions (P-D2). Additionally, the Police also collaborate with others outside the force if a crime has taken place (P-D3). Indeed, this collaboration does not only happen on a national level but mostly on an international level in order to deal with this threat, meaning Police agencies often work with others across the globe (P-D2, P-W3), despite their priorities remaining at home (P-W2). A

global approach is needed in this case because "*from the moment you go online you are internationally connected*" (P-D3). Despite the rise of several national illegal trading markets, international business prevails. The Police therefore understand that "*it is almost the default that we have to work internationally*" (P-D2). Coalitions of Police forces have therefore been formed to establish common strategies instead of working as individual countries (P-D2). Collaboration is so important as part of policing operations that it was collectively mentioned 226 times in the drug and wildlife documents analysed in the Reporting section.

In these kinds of collaborative environments, especially with such sensitive information and sectors participants might not be familiar with, trust is key. Just as the Police have been establishing trust relationships with other agencies and externals over years of working together, they are also trying to create a culture where individuals share information with them when they come across it and have confidence in them to take further action (P-D2). However, many organisations do not yet trust one another, as experts with Police backgrounds sometimes judge private actors' approaches as "*too cavalier*" and wish undercover work was reserved for people who have received proper Police training (P-W3). These collaborations therefore remain fragile and dependent upon individual forces' experience with and trust in other policing actors.

Police agencies are increasingly involved and collaborating on cybercriminal matters, including the policing of online illegal drug and, to a lesser extent, wildlife trade. Due to the interjurisdictional aspect of online trade, it is no longer optional for various forces to come together for policing purposes. As such, large international agencies have coordinated global interventions and national forces have sought the expertise of local and specialised agencies. However, trust remains to be built and strengthened between Police agencies and external policing actors, as they realise they can benefit from each other's skills and expertise. As such, the UNODC advocates for more public/private partnerships be forged between Internet Service Providers, technology companies, and shipping and mailing companies in response to rising illegal web-based sales (UNODC, 2021c).

The answer to our fourth research question is therefore that increased collaborations between the Police and other policing actors in the public and private realms, for intelligence and expertise sharing, information gathering, operation conducting, and reporting, can further increase the effectiveness of online illegal drug and wildlife trades policing. These collaborations are at the centre of the policing script presented in the Discussion chapter, as it is argued understanding the goals and skills or other entities will spur further collaborative Police interventions in the future.

4.4 Conclusion

This chapter presented an exploratory study into the evolving role of the Police and their contribution to the policing of the online illegal trades of drugs and wildlife through the use of expert interviews and the content analysis of Police agency publications.

The Police participate in the policing of these online illegal trades by receiving intelligence from other policing actors about potential illegal trades and traders, gathering additional information about them, conducting direct interventions to stop these trades, such as arresting traders and seizing their stocks, and reporting on their and others' interventions.

This chapter was divided in three parts: the first part presented findings about the Police agencies involved in this policing; the second part then analysed the activities the Police perform and how these differ between the policing of online illegal drug and wildlife trades; and the third part discussed how the Police can be more effective in this type of policing in the future.

While the presence and activity of the Police in the policing of drug trade, both offline and online, cannot be contested, this chapter has shown that their role is different and more reserved in the policing of online illegal wildlife trade. This is likely due to several reasons, from non-specialised Police agencies' lack of expertise in wildlife matters to the location of such trades on legal platforms as opposed to the Darknet. Indeed, as will be shown in the next chapter, administrators on trading sites and moderators on social media platforms are responsible for ensuring the legitimacy of these legal platforms, instead of the Police. Collaboration is therefore paramount for the policing of these trades, not only with other Police agencies as shown in this chapter and the previous literature review, but also with legal platforms and private organisations which possess complementary resources and skills necessary in this policing, as shown in this thesis' policing script. The legal online platforms these trades happen on and their administrators' and moderators' role in the policing of online illegal drug and wildlife trades are explored in the next chapter.

5 Legal online platforms

Beyond Darknet markets which are mainly regulated by the Police, numerous news and academic articles have pointed to the increased trade of illegal drugs on legitimate websites and social media applications, as these platforms are more broadly accessible than Darknet markets and offer convenience and protection to their users (Babb, 2014; Thanki and Frederick, 2016; EMCDDA and Europol, 2019; Moyle et al., 2019). Administrators and moderators themselves are responsible for ensuring the legitimacy of these platforms. Considering these increased trades on their sites, Facebook, Twitter, and Google founded the group Tech Together to Fight the Opioid Crisis in 2018 alongside the Center for Safe Internet Pharmacies (CSIP, 2021a), aiming to reduce drug trade, raise awareness, and provide help to fight users' addictions (Facebook, 2018b).

Alarming volumes of illegal wildlife trade on legal platforms have also led to the creation of the Coalition to End Wildlife Trafficking Online in 2018 including sites, such as eBay, Etsy, Facebook, Instagram, and many more, coming together to reduce illegal wildlife trade on their platforms (Coalition to End Wildlife Trafficking Online, 2020). Although it is not a part of the current Coalition, Gumtree was a member of the Coalition's precursor framework formed in 2016 to provide legal platforms with unified wildlife trade policies. eBay and Etsy were also members of a national group working to reduce this type of trade, the United States Wildlife Trade Alliance, years earlier (eBay, 2016c).

We therefore have much to gain from researching both of these products as part of the same study, gathering complementary insights to provide useful strategies for their future individual policing. The activities of legal online platforms in both realms are explored and compared in this chapter. It is unclear in the Internet pharmacies group, but the wildlife coalition theoretically involves the use of unified policies for trading websites and social media applications in order to restrict the trade of illegal wildlife products and implement enforcement mechanisms for these rules (TRAFFIC WWF IFAW, 2017; Coalition to End Wildlife Trafficking Online, 2020). The Police and specialised non-profit organisations have also identified several factors as necessary to reduce illegal trade on legal platforms. These factors include enforcement, as monitoring and detection cannot be successful without implementation and penalties (IFAW, 2018a); crowdsourcing detection efforts to platform

users (IFAW, 2014b; Coalition to End Wildlife Trafficking Online, 2020), as they are more likely to come across content violating platforms' policies (IFAW, 2012; EMCDDA and Europol, 2019); and consumer education about the platforms' policies and illegal trade as a whole, as they cannot be expected to know as much as experts, especially in matters as complex (IFAW, 2014a; EMCDDA and Europol, 2017a; IFAW, 2018a; EMCDDA and Europol, 2019; Coalition to End Wildlife Trafficking Online, 2020).

Indeed, while both types of online trade platforms, surface and Dark, have put in place policies to restrict the type of trade permitted on them, these rules can be difficult to enforce. Trade restrictions are more often thought about in the case of legal platforms ensuring they remain legitimate and do not compromise the safety of their users or their reputation. Various items are therefore prohibited for trade on these sites, some because of their illegality and others in response to public opinion (eBay, 2008a). It is understood that restricting the legal supply for a product or service will increase its illegal supply, as was the case for prescription opioids which became more significantly traded on the Darknet between 2014 and 2016 following such restrictions (Martin et al., 2018a). Unlike what one might picture, Darknet markets however are not marketplaces that allow any and all products and services to be traded. While some illegal products are bought and sold on these marketplaces, several restrictions have also been put in place to reflect the values of their users. Indeed, some Darknet markets do not allow the posting of child sexual exploitation materials (Cyjax, 2018c) or the trade fentanyl, a very potent opioid substance which rapidly made its way to the top traded drugs on the Darknet and has been responsible for many deaths (Flashpoint, 2017a; Martin et al., 2018a), including during the COVID-19 pandemic (The Economist, 2021). In more general terms, however, policies restricting online illegal trade have not received much attention, as the few studies which touch upon online trade rules and regulations are focussed on the extent to which users are aware of, read, and understand privacy rules (Vila et al., 2003; Pollach, 2007; McDonald and Cranor, 2008; Turow et al., 2008; Tsai et al., 2011; Steinfeld, 2016). Although several forums and marketplaces have published guidelines about what components online retail policies should include, no study could be found, whether relating to offline or online markets, about the presence, importance, and content of these trade policies, which this thesis argues are indispensable in the broader policing apparatus.

The aims of this study are therefore to understand the ways in which legal online platforms are participating in the policing of online illegal drug and wildlife trade on their sites to better situate this group in the cyber policing classification and policing script devised in the Discussion chapter.

Platforms in this thesis refer to any type of legal online platform, including trading websites, auction websites, and social media and instant messaging applications. Darknet markets are not included in this analysis as they permit some illegal trade and are not subject to the same rules as legal platforms.

Research for this chapter was conducted by analysing the content of 11 online platforms' illegal drug and wildlife trade policies (eBay, Etsy, Facebook, Freeads, Gumtree, Instagram, Pets4Homes, Preloved, Twitter, WeChat, and WhatsApp) and interviewing two legal online platform administrators. Although this thesis focusses on wildlife trade more generally, most of the above policies and interviewees specialised in and mentioned animal trade.

This chapter therefore focusses on legal online platforms while investigating this thesis' broad research questions:

1. Are legal online platforms involved in the policing of online illegal drug and wildlife trades?
2. What activities do legal online platforms perform?
3. How similar or different are the legal online platform actors and activities involved in the policing of online illegal drug and wildlife trades?
4. How can this type of policing be rendered more effective in the future?

In order to answer the aforementioned questions, this chapter is divided in three parts, each one focussing on different research questions. The first part presents findings about the legal online platforms involved in the policing of online illegal drug and wildlife trades; the second part then analyses the activities these online platforms perform and how these differ between the policing of online illegal drug and wildlife trades; and the third part discusses how legal online platforms can be more effective in this type of policing in the future.

5.1 Legal online platform actors

Unlike for the policing of Darknet markets for which the Police have a prominent role, trade on legal platforms is under the responsibility of the platforms themselves, and specifically their administrators and moderators. As such the Police have required support from these platform administrators and moderators in order to disrupt online illegal drug and wildlife trades on their sites.

Legal platforms include many different sites from legitimate trading websites, to social media and instant messaging applications. Some of these platforms are entirely dedicated to trade, while others are centred around communication, which leads to trade in certain cases. Many are broad platforms that house trade in a range of products, while others are specialised, such as online pet shops and online pharmacies. This category is therefore a broad one, as many platforms house online trade, some of which has the potential to be illegal, and they have to take action to reduce such illegality.

It should however be noted that whichever form these platforms take, their focus on security is only secondary. Indeed, although they are responsible for ensuring the legitimacy of their sites, their main line of work remains trade or communication, not security. Nonetheless, security has gained prominence in their work, as both the Police and the public have advocated for better control in light of their use for illegal trade. Legal platforms are therefore a prominent policing actor for this type of crime. Specifically, the administrators who run these legal platforms and are in charge of monitoring them and have a duty to identify and remove any illegal trading happening on their site. Failure to do so can result in the Police or private organisations contacting the platform to signpost the illegal content and request its takedown (P-W2; LP-W1) and in platform users voicing their dissatisfaction about the way the sites are run (LP-DW1). Similarly, moderators are employed by or volunteer to regulate content posted on social media platforms, which can require removing posts, images, or videos which violate the law or platforms' rules (Button, 2020).

The answer to our first research question is therefore that legal online platforms, in their many shapes and forms, are prominent policing actors for this type of crime, acting as the first line of defence when illegal products are listed on their site. Legal online platforms are

therefore the second part of the cyber policing classification devised in the Discussion chapter. The following section analyses the specific activities they perform as part of this policing.

5.2 Legal online platforms activities

Insights from interviews and content analysis have highlighted five main activities performed by legal online platforms to disrupt illegal drug and wildlife trades on their sites: 1) Trade policies publishing, 2) Platform monitoring, 3) Information receiving, 4) Content removing and user blocking, and 5) Awareness raising. These are analysed in turn and the specific activities involved in policing both products are emphasised where they differ.

5.2.1 Trade policies publishing

The first step in preserving the legitimacy of their site and avoiding sanctions (POI-W2), is for legal platforms to publish trade policies – rules which are placed on their sites about what users are or are not allowed to post (LP-W1; LP-DW1). These policies can take several forms, such as a simple page of text detailing these rules, including more or less information about potential consequences from breaking them (LP-W1; LP-DW1). More interactive systems have also been put in place whereby messages pop-up on vendors' screens as they submit a listing that is flagged as potentially illegal due to its wording or lack of appropriate documentation (POI-W1) or on buyers' screens as they search for certain keywords linked to illegal items (POI-W2). Indeed, it is complex for traders to know and understand all the relevant policies in place on specific sites, as these policies often encompass a lot of information, but this understanding has been argued to be up to traders rather than the platforms they operate on (LP-DW1). Such interactive warnings can therefore help users in these cases. These policies can be particularly complex to devise and understand in the case of global platforms, which might have to navigate between different legislative environments and products and services which are legal in some countries and not others (LP-DW1).

Several legal platforms reported working on and improving their policies with the help of specialised organisations, forming cross-sector groups to ensure a zero-tolerance policy for

illegal activity (LP-W1; POI-D6). Such collaboration was in fact deemed the best strategic decision for one of the platform administrators interviewed, as their non-profit partner possessed deep knowledge the administrator didn't and was able to assist them in the process. This allowed them to soar to new heights among their community, which the administrator admitted they wouldn't have been able to do on their own (LP-W1). Another platform mentioned not cooperating with such organisations in the past, as it operated in a "*do it yourself*" culture, but these collaborations are slowly starting to emerge (LP-DW1). In any case, interviewees reported not working with other legal platforms, as competition remains a prominent theme in the private sphere (LP-W1; LP-DW1; POI-W5).

The comprehensiveness of illegal drug and wildlife trade policies of various websites, social media, and instant messaging applications is now evaluated. In this study, comprehensiveness is defined by the length, precision, language, reference to enforcement mechanisms, and additional information provided by legal platforms' policies regarding illegal drug and wildlife species and products. Reference to enforcement mechanisms and additional educational information were characteristics derived from Police descriptions of what good policies should entail contained in this chapter's Introduction (IFAW, 2014a; EMCDDA and Europol, 2017a; IFAW, 2018a; EMCDDA and Europol, 2019; Coalition to End Wildlife Trafficking Online, 2020). A policy's length, precision, and language are also argued to participate to its comprehensiveness. Indeed, although length gives an indication of how much a platform has written about the subject and this might indicate precision and the inclusion of additional relevant information not contained in shorter policies, this characteristic does not encompass the kinds of words used and their meaning, which also need to be taken into account. These characteristics are evaluated in turn in the remainder of this section.

The length of trade policies regarding both drug and wildlife products is first evaluated. The nine investigated legal platforms all mentioned drugs in their trade policies, although the degree to which they did so differed. Indeed, the number of words used to describe the platforms' policies about drug trade varied from two to 282. Four policies used 20 words or fewer, three used between 35 and 125 words, and only two used more than 200 words.

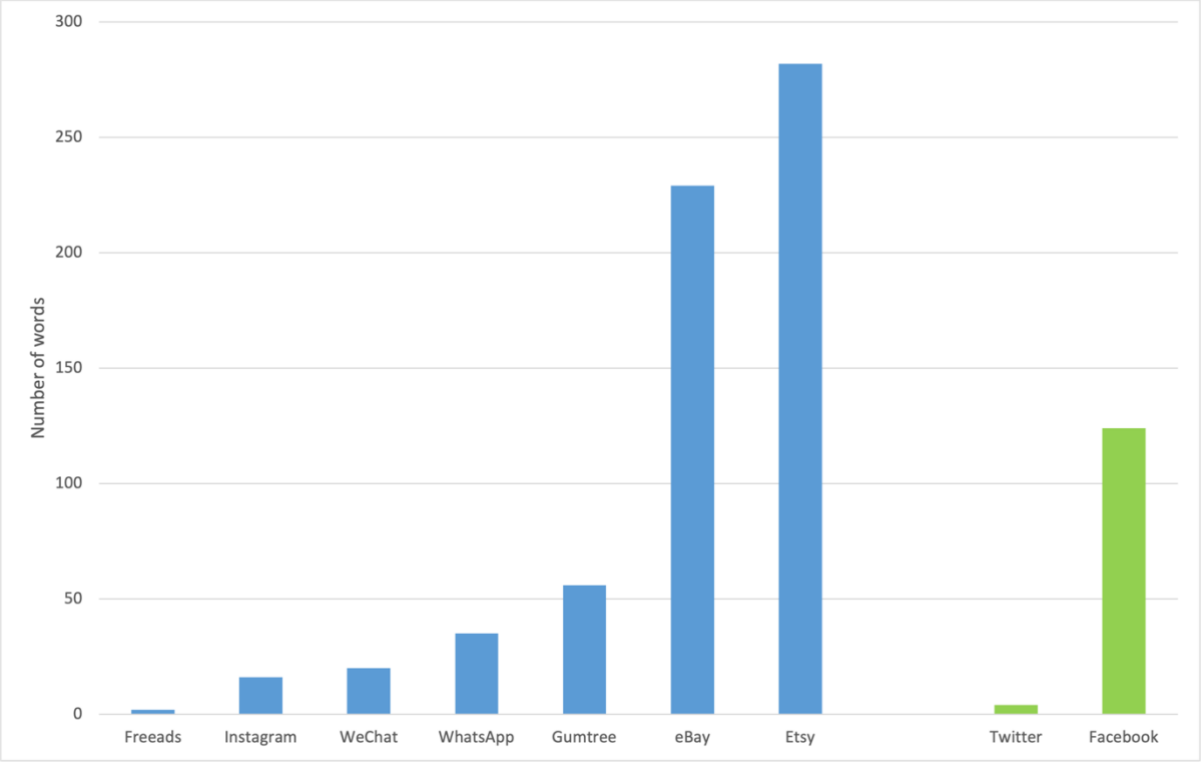


Figure 5.1: Number of words written about drugs in each online platform's trade policy The platforms in blue are not part of groups working to reduce online illegal drug trade and the ones in green are or have been

Involvement in a group aimed at reducing illegal drug trade online therefore did not mean having lengthier policies for Twitter and Facebook. However, comparing the volume of words for each group is not very insightful here, as the number of platforms in each category is not balanced, unlike the wildlife trade policies below. However, it should be noted that most trading websites, Freeads excluded, had lengthier policies than social media and instant messaging applications.

Similarly, the ten investigated legal platforms all mentioned wildlife in their trade policies. However, the number of words used to describe illegal wildlife trade policies varied from 15 to 550. Six policies used 60 words or fewer, three used between 180 and 194 words, and eBay used more than 500 words.

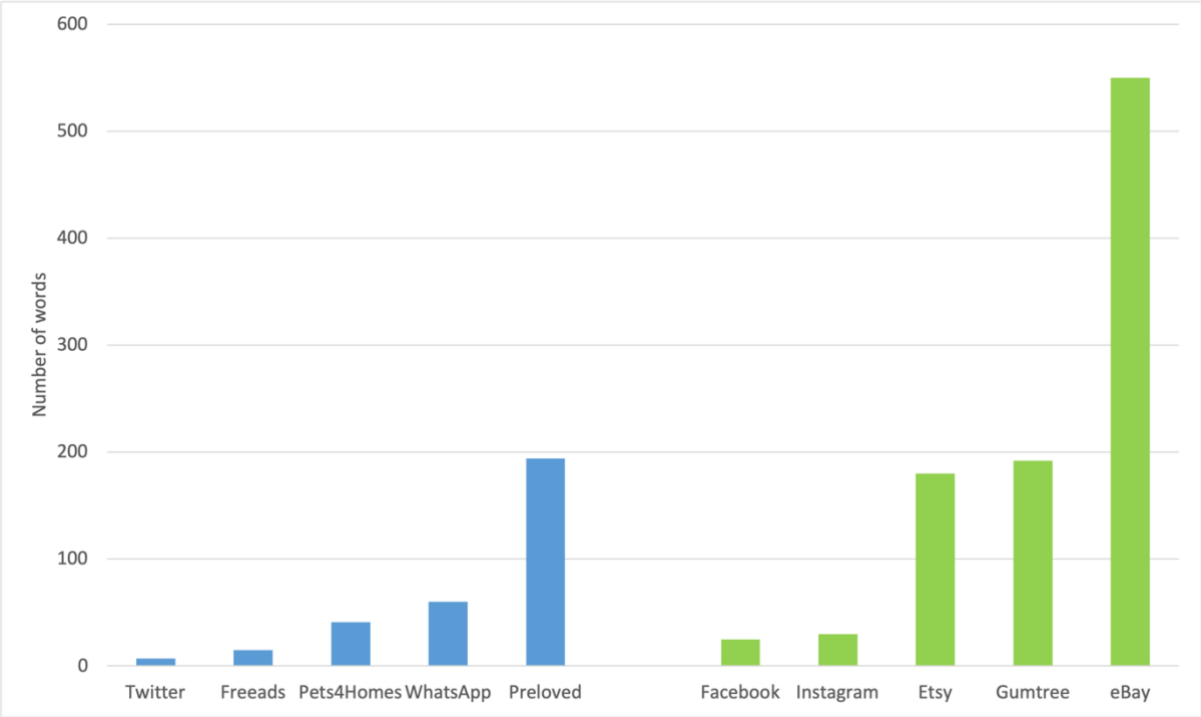


Figure 5.2: Number words written about illegal wildlife in each online platform's trade policy The platforms in blue are not part of groups working to reduce online illegal wildlife trade and the ones in green currently are or have been

Members of groups aiming to reduce online illegal wildlife trade were likely to have more words allotted to describing illegal wildlife species and products in their policies. Indeed, group member had an average of 195 words per policy and a total of 977 words across all members, compared to 63 average words per non-member policy and a total of 317 words in that sub-group. In the member group, trading websites also had lengthier policies than their social media and instant messaging counterparts. This difference generally applies but is less stark in the non-member group, as WhatsApp has the second highest wordcount in that sample.

Overall, the length of online illegal drug and wildlife trade policies therefore differed. Not only was the range of illegal wildlife trade policy lengths wider but the minimum and maximum policy lengths were also significantly higher than for drug policies. This potentially implies that the illegality of wildlife is less understood by the public than that of drugs, more difficult to define, and requires more words and pieces of external information to explain and justify. Additionally, unlike drug policies for which membership to a group aiming to reduce illegal trade did not have an obvious impact, group membership had a positive impact on illegal wildlife trade policies. Indeed, the five group members wrote 76% of the total words included in the investigated wildlife trade policies. While this does not speak to the content of these policies, it seems group members were either given access to or actively sought out more information to include in their policies to prevent illegal wildlife trade on their sites. Additionally, across both products, trading websites' policies were lengthier than those of social media and instant messaging applications, potentially explaining the growing amounts of trade on the latter as they were initially designed for communication rather than trade. They were therefore less prepared than their trading website counterparts for these challenges.

Beyond the strict number of words written about illegal drug and wildlife products in the investigated legal platforms' trade policies, the content of these policies, also differed from one platform to another.

In the case of drugs, WhatsApp was the only platform not to provide any information about why certain drug products were not allowed on their site, while most other platforms justified these restrictions by explaining they wanted to protect their users and abide by the law. Policies across platforms also varied in their precision. The least descriptive policy came from Freeads, which only mentioned that all advertisements needed to be legal in the UK and that additional restrictions applied to protect families, including 'no pharmaceuticals'. On the other end of the spectrum, the most precise policy was available on eBay, divided across two specific policies - one about 'illegal drugs and drug paraphernalia' and one about 'prescription and over-the-counter drugs'.

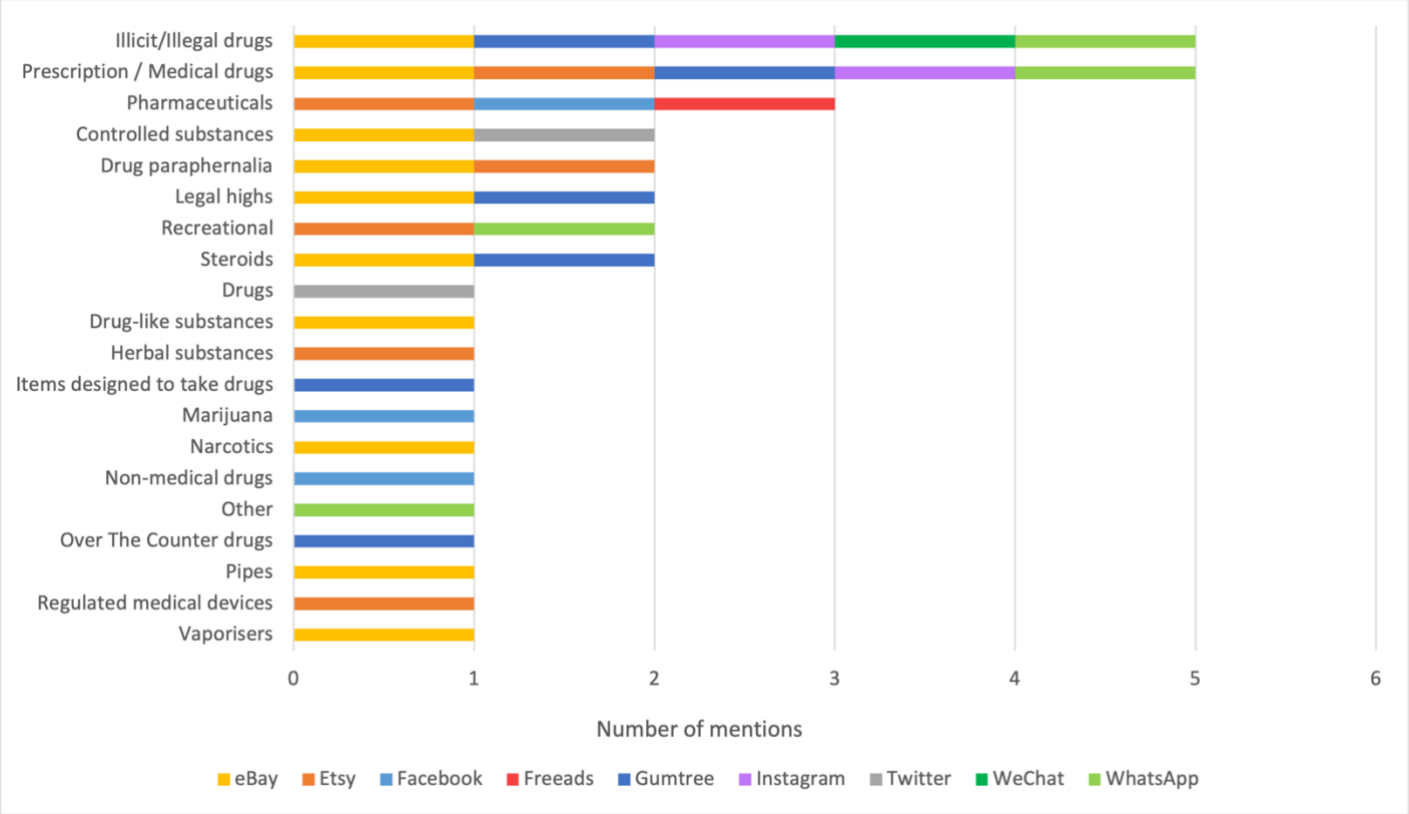


Figure 5.3: Number of mentions of each illegal drug-related keyword in online platforms' trade policies

Only two of 20 keywords, 'Illegal / Illicit drugs' and 'Prescription / Medical drugs' were mentioned in five different policies, 30% were mentioned in two or three policies, and 60% were only mentioned in one, showing the breadth of terms used to refer to drug products, with more or less precision. Additionally, two of the nine platforms, Freeads and WeChat, only mentioned one keyword in their policies, 45% of platforms mentioned between two and four keywords, Etsy and Gumtree mentioned six, and eBay mentioned ten.

In the case of wildlife, Pets4Homes and WhatsApp were the only two online platforms not to provide any information about why certain wildlife products were not allowed on their platform, while most other platforms justified these restrictions by explaining they wanted to protect their users, wildlife, and abide by the law. Policies across platforms varied in their precision. The least descriptive policy came from Freeads, which only mentioned that all advertisements needed to be legal in the UK and that additional restrictions applied to protect pets so 'prohibited species' could not be offered. This appeared in the same bullet point as 'banned breeds' with no additional explanation about these terms. Unlike Pets4Homes and Preloved, the site also involves the trade of non-live animal products, so the term species appears reductive. Although it wasn't lengthy, the most precise policy was available on WhatsApp.

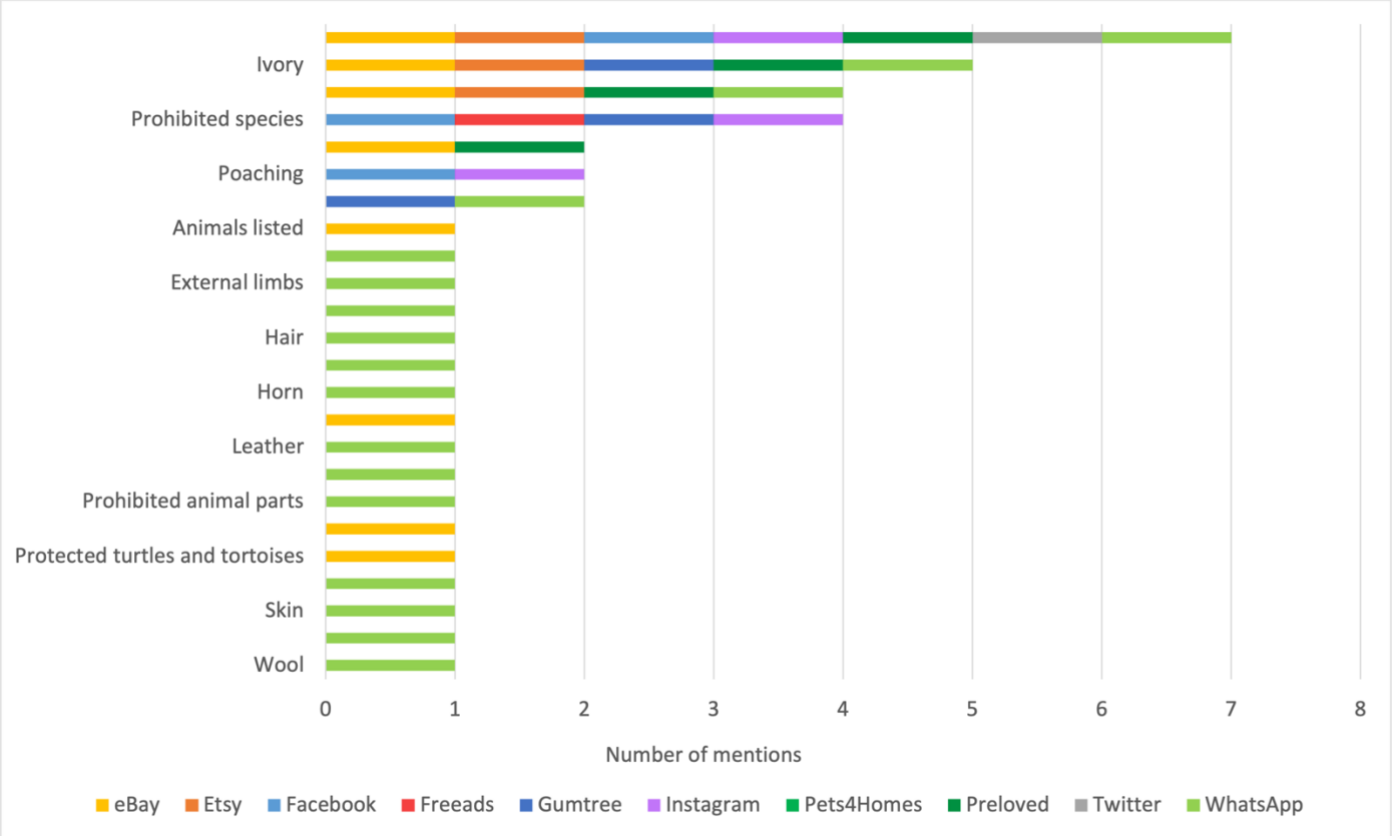


Figure 5.4: Number of mentions of each illegal wildlife-related keyword in online platforms' trade policies

Only one of 24 keywords, 'Product or part of endangered / threatened / protected animals' was mentioned in seven policies, three were mentioned in four or five, two were mentioned twice, and 76% were only mentioned once. Additionally, Twitter and Freeads only mentioned one keyword in their policies, 25% of platforms mentioned three or four keywords, eBay mentioned eight, and WhatsApp mentioned 17. Pets4Homes did not include policies restricting any specific product trade on their platform, and instead only provided information about what documentation vendors needed to provide in order to advertise live animals, it therefore does not appear in the above graph.

Overall, all but one platform justified their illegal drug trade policies to their users and all but two justified their illegal wildlife trade policies. All of these justifications included abidance by the law in the case of drug policies, but only 80% of wildlife policy justifications did. However, four wildlife policies mentioned precise rules and regulations restricting these trades, while only one drug policy did. Drug trade policies across platforms consisted of a total of 20 keywords, compared to 25 keywords across illegal wildlife policies. The most-mentioned drug-related keyword was included in five policies and the most-mentioned illegal wildlife-related keyword in seven. However, both of these choices were very broad and imprecise, as they were often left undefined. 60% of drug-related keywords were only mentioned in one policy, compared to 76% of illegal wildlife-related keywords. In both cases, two drug and illegal wildlife trade policies only used one keyword, and Pets4Homes did not restrict any illegal wildlife product but instead gave terms under which items could be listed. Finally, the platforms which listed the most keywords were eBay with ten keywords throughout its drug trade policy and WhatsApp with 17 keywords throughout its illegal wildlife trade policy. Overall, four keywords were included on average in both illegal drug and wildlife trade policies. However, the average number of keywords used by group members was three in their illegal drug trade and eight in their illegal wildlife trade policies, compared to four and one respectively for non-group members. This is counting the fact that WhatsApp, holding the record for using the most used wildlife-related keywords in its policy, is a non-group member therefore explaining large discrepancies in between platforms.

In light of these differences, it is recommended that policies include more precise keywords in order to send the right message to users (IFAW, 2014c, 2014b). Indeed, while many of the keywords reported in this investigation referred to the same thing, such as 'Drug paraphernalia' and 'Items designed to take drugs', they were purposefully kept separate to show just how many keywords users are exposed to and need to navigate through if and when they read through these policies. Although certain platforms might allow more or fewer products to be traded than others, an effort should be made through the illegal trade reduction groups mentioned earlier in this chapter for the keywords used to be consistent and explained across platforms. This would ensure there is no doubt or confusion in users' minds and they do not choose to trade on one platform over another because their descriptions were not as explicit. Additionally, in the case of drug trade policies, special attention should be paid to New Psychoactive Substances or legal highs, which are seldom mentioned in these policies, as these are likely not considered as 'illicit / illegal drugs' by users and have been increasingly traded on the surface web (EMCDDA and Europol, 2017a, 2019). Finally, while only products not allowed for trade were investigated as part of this study, it is also important for legal platforms to clearly enumerate the products that are allowed. Police and specialised organisations also emphasised the importance of collaboration in the fight against online illegal trade (EMCDDA and Europol, 2017a; Europol, 2018c; IFAW, 2018a), so legal platforms not currently part of these groups are encouraged to join them or create their own in order to learn from others and refine their policies together.

The number and type of keywords used therefore varied between platforms, group and non-group members, rendering illegal drug and wildlife trade policies more or less precise from one platform to the next. These keywords were also linked together by general language used to express restriction.

Surrounding these keywords, the language used in drug trade policies was also more or less expressive across platforms, both in terms of its strength and its volume in each policy.

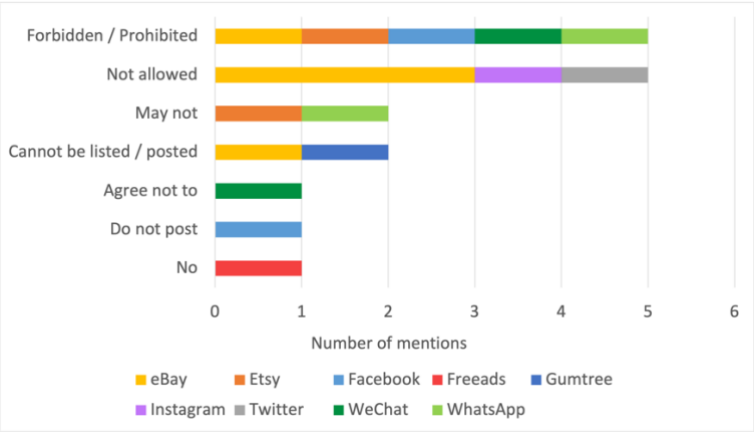


Figure 5.5: Number of restrictive expressions used in online platforms' illegal drug trade policies

The most used expression included in 56% of the policies under review was variations of 'Forbidden / Prohibited'. 'Not allowed' was then included five times by three different platforms, 'Cannot be posted / listed' and 'May not' were both used twice, and 'Agree not to' 'Do not' and 'No' only once. From the platforms' perspective, eBay used three different expressions to restrict trade across its policies, while half of the remaining platforms used one restricting expression and the other half used two.

The language used in wildlife trade policies also varied in its strength and volume across platforms.

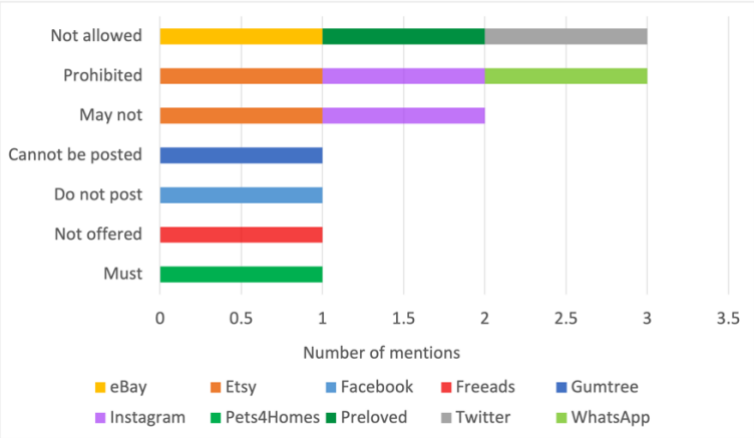


Figure 5.6: Number of restrictive expressions used in online platforms' illegal wildlife trade policies

Variations of 'Not allowed' and 'Prohibited' were each included in 33% of the policies under review. 'May not' was used in two policies, and 'Cannot be posted', 'Do not' and 'Must' only in one each. Etsy and Instagram used two different expressions to restrict trade in their policies and the remaining eight policies only used one restricting expression each.

These expressions used both positive / negative, and active / passive formulations.

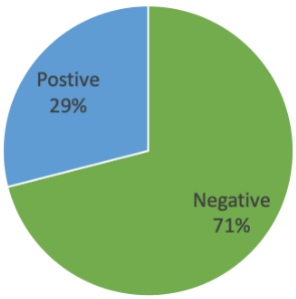


Figure 5.7: Proportion of negative and positive language used in online platforms' illegal drug trade policies

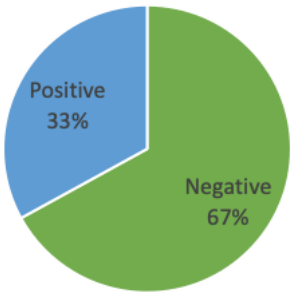


Figure 5.8: Proportion of negative and positive language used in online platforms' illegal wildlife trade policies

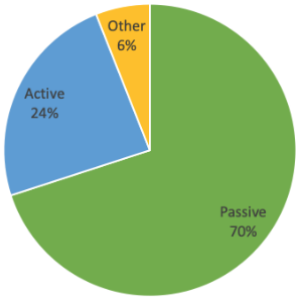


Figure 5.9: Proportion of passive and active language used in online platforms' illegal drug trade policies

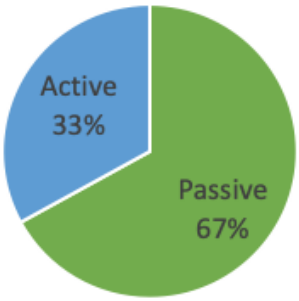


Figure 5.10: Proportion of passive and active language used in online platforms' illegal wildlife trade policies

Most expressions used negative language either including ‘not’ or ‘no’, except for the five uses of ‘Forbidden / Prohibited’ in drug trade policies and three in wildlife trade policies, which only represented 29% and 33% of the used expressions across policies respectively. While Freeads’ simple use of ‘no’ cannot be qualified as either active or passive, the majority of expressions also used passive language including past participles, except for ‘you may not’, ‘you agree not to’, ‘do not’, and ‘must’ which referred to direct actions by users and only represented 24% and 33% of the used expressions across drug and wildlife trade policies respectively.

Overall, illegal drug trade policies across platforms were more likely to use several expressions to restrict trade on their sites, with 56% of legal platforms using two or more expressions, compared to only 20% in the case of illegal wildlife trade policies. Of these expressions, ‘Forbidden / Prohibited’ was included in five illegal drug trade policies, followed closely by ‘Not allowed’ mentioned in three. However, both expressions were used by only three platforms in their illegal wildlife trade policies. If it is agreed that ‘Forbidden / Prohibited’ is a level of restriction above ‘Not allowed’, legal platforms are less likely to use strong language in their illegal wildlife compared to illegal drug policies. This discrepancy in the use of strong language comes even as TRAFFIC, WWF, and IFAW (2017) used the word ‘prohibited’ in bold and underlined in their sample policy framework to be used by Coalition to End Wildlife Trafficking Online members on their platforms. More restrained language was therefore used in illegal wildlife trade policies, although it is unclear whether this could have an incidence on the volume of these trades on legal platforms, as illegal traders are unlikely to read these policies and focus on these distinctions. The remaining expressions were similar across both categories of policies. Another difference in language is that illegal wildlife policies were slightly more positive and active than their drug counterparts, though that difference wasn’t significant. Although the terms used in illegal wildlife policies are weaker, they are therefore more likely to involve direct actions by users, which is recommended for its simplicity with regards to legal or policy language (Charrow and Erhardt, 1986; Good, 1989; Williams, 2005). They are also less likely to use negation such as ‘no’ and ‘not’. Additionally, 43% of illegal wildlife trade group members’ policies included active language, compared to 20% for non-members.

Language used to restrict illegal drug and wildlife trade therefore varied between platforms, group and non-group members, not only in its strength but also in its volume and formulation. Following such restrictions, enforcement and reporting mechanisms were used in order to punish any policy breaches.

Enforcement and reporting mechanisms were often mentioned in illegal drug trade policies if the above prohibited and restricted items were not respected by users. WeChat was the only platform not to provide any information about the consequences of breaking their trade policies. While the other eight platforms all mentioned this information, only six included it right above or below their policies. Facebook and WhatsApp had separate pages for these matters. The consequences of rule breaking also varied from one platform to the next.

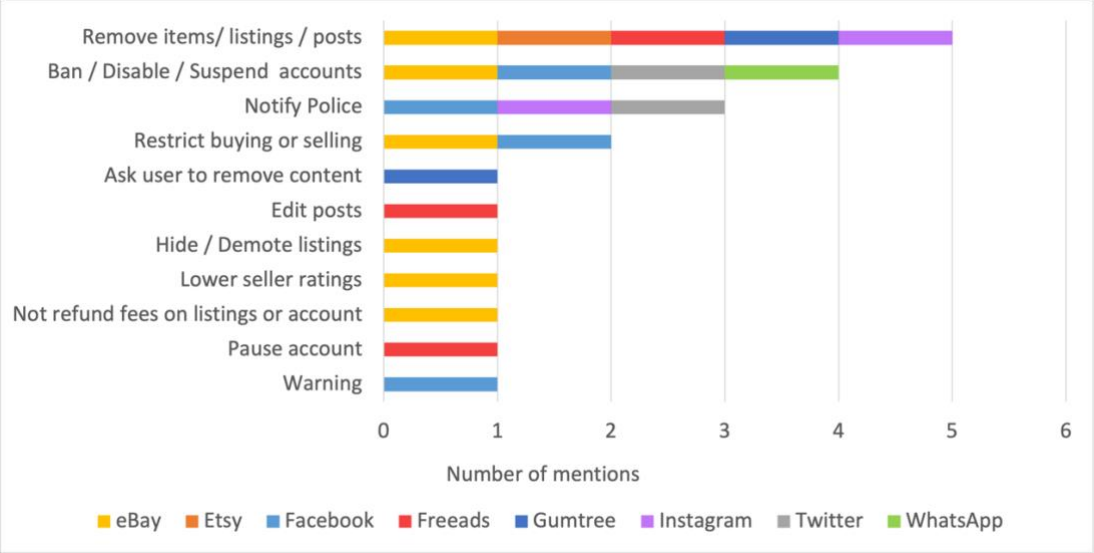


Figure 5.11: Number and kind of enforcement mechanisms mentioned in online platforms' illegal drug trade policies

Out of 12 enforcement mechanisms mentioned in legal platforms' drug trade policies, 'Remove items / listings / posts' was mentioned five times and 'Ban / Disable / Suspend accounts' four times, making these two interventions the most likely as a response to illegality. These interventions are explored further in a later section. eBay once again shows itself to be a leader in this sample by mentioning more enforcement mechanisms than any other platform, including six in its policy, compared to four for Facebook, one for WhatsApp,

and two or three for the other six platforms. For the platforms including the most enforcement mechanisms, it was noted that the consequence of violating their policies would be dependent on the severity of the violation and the previous history of the user in question, therefore creating additional degrees of enforcement and justifying their more numerous mechanisms (LP-DW1).

Additionally, all platforms but WhatsApp provided Reporting mechanisms in case users came across content violating their illegal drug trade policy, which the administrators might not have detected. WhatsApp had a similar policy, though only aimed at reporting spam messages on their application. Of the remaining eight platforms which implemented this mechanism, only three included information about it directly in their policies. The other five included it in other related pages specifically about reporting posts and content, and therefore included other reasons why reporting might be needed.

Similarly, all ten legal platforms included information about the enforcement mechanisms related to the illegal wildlife trade policies in place on their sites. Most of this information was included right above or below theses policies, but Facebook and WhatsApp had separate pages for these matters. The consequences of these breaches also varied from one platform to the next.

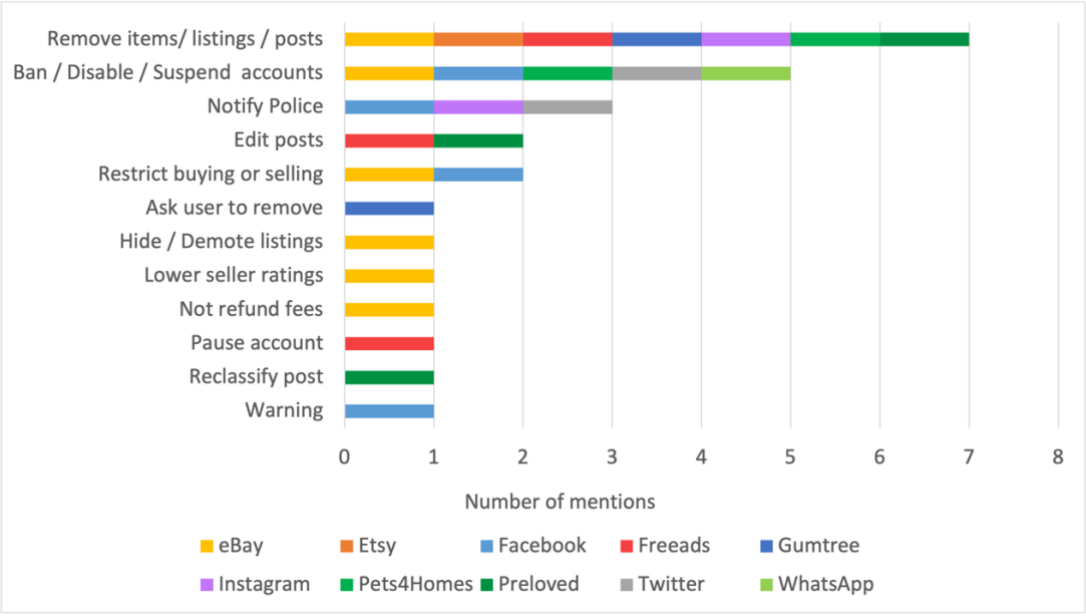


Figure 5.12: Number and kind of enforcement mechanisms mentioned in online platforms' illegal *wildlife trade policies*

Out of 12 enforcement mechanisms mentioned in legal platforms' wildlife trade policies, 'Remove items / listings / posts' was mentioned in seven policies and 'Ban / Disable / Suspend accounts' in five, making these two interventions the most likely as a response to illegality in the case of wildlife trade too. Once again, eBay mentioned the most types of enforcement mechanisms, including six in its policy, compared to four for Facebook, one for WhatsApp, and between two and three for the other seven platforms. For the platforms referring to the most mechanisms, it was noted that the consequence of violating their policies would be dependent on the severity of the violation and the previous history of the user, therefore creating additional degrees of enforcement and justifying their more numerous mechanisms (LP-W1; LP-DW1).

Additionally, all legal platforms but WhatsApp provided reporting mechanisms in case users came across content violating their illegal wildlife trade policy, which the administrators might not have detected. WhatsApp had a similar policy, though only aimed at reporting spam messages on their site. Of the remaining nine platforms which implemented this mechanism, only three included information about it directly in their policies. The other six included it in other related pages specifically about reporting posts and content, and therefore included other reasons why reporting might be needed.

Overall, WeChat was the only platform not to include any enforcement information in its drug and wildlife trade policies. This lack of threat of enforcement might therefore explain the amount of trade witnessed and reported on the application (WJC, 2017a). Six of the eight illegal drug trade policies included this information directly in their policy, while the other two had separate pages reserved for such matters, compared to five and three for illegal wildlife trade policies. As these mechanisms were site-wide, the content is similar for both illegal drug and wildlife trade policies. Indeed, both categories mentioned a similar number of enforcement mechanisms, and the most-mentioned mechanisms across both categories was 'Remove items / listings / posts', followed closely by 'Ban / Disable / Suspend accounts'. Additionally, 59% of drug trade policies' and 54% of illegal wildlife trade policies' enforcement mechanisms were only mentioned by one platform. In both cases, eBay included six mechanisms and Facebook four in their policies, while WhatsApp only included 'Ban / Disable / Suspend accounts'. The reason for this might be that unlike trading websites and other social

media applications where users can post content, WhatsApp is solely used as a communication platform and most of the other mechanisms therefore do not apply. Overall, 23 enforcement mechanisms were mentioned across all drug trade policies and 28 for illegal wildlife ones. Across both categories, group members included three mechanisms on average, compared to two for non-members. Additionally, all online platforms but WhatsApp included information about reporting mechanisms for users, if they came across content violating their policies before their detection systems. This anomaly might be due to WhatsApp not being used to post content but to communicate. However, it might be useful to report users not only for spam but also for trying to sell illegal products from their accounts. Only three reporting policies in both categories were included directly in the platforms' wider policies, while the others were general reporting mechanisms used by the site and therefore included other reasons for flagging this content. It should be noted that some legal platforms are more measured about citing their enforcement mechanisms, choosing instead to keep them more implicit and not threaten users with certain consequences if they do not abide by their policies (LP-W1). Indeed, they would not take any drastic enforcement action lightly, instead ensuring they have all the information necessary about the listing's illegality before intervening (LP-DW1).

While enforcement and reporting mechanisms have been largely been put in place by the legal platforms in this study, the placement of these mechanisms is inconsistent across platforms. Not only should platforms not currently possessing such mechanisms put them in place, but it is recommended they are located near the policies they are aimed to enforce. Certain legal platforms have separate policies for each type of trade, such as eBay (2020a, 2020b, 2020c), but other platforms investigated in this study put all their policies together on the same page. In both cases, it would be easy to add these mechanisms on the same page instead of keeping them separate (though separate pages could also be kept for thoroughness). This will make it easier for users to get the full picture all in one place. Additionally, this information should stand out on these pages, as it was sometimes difficult to locate either at the beginning or at the end of policy pages. Putting them in bold, colour, in a box, or under an expressive title about consequences of policy breaches would therefore make them easier to spot.

In order to make clear what products were restricted, or to allow for further queries, some legal platforms also provided additional information to their users.

All but two platforms provided additional drug-related links and resources to their users, though this information took different forms.

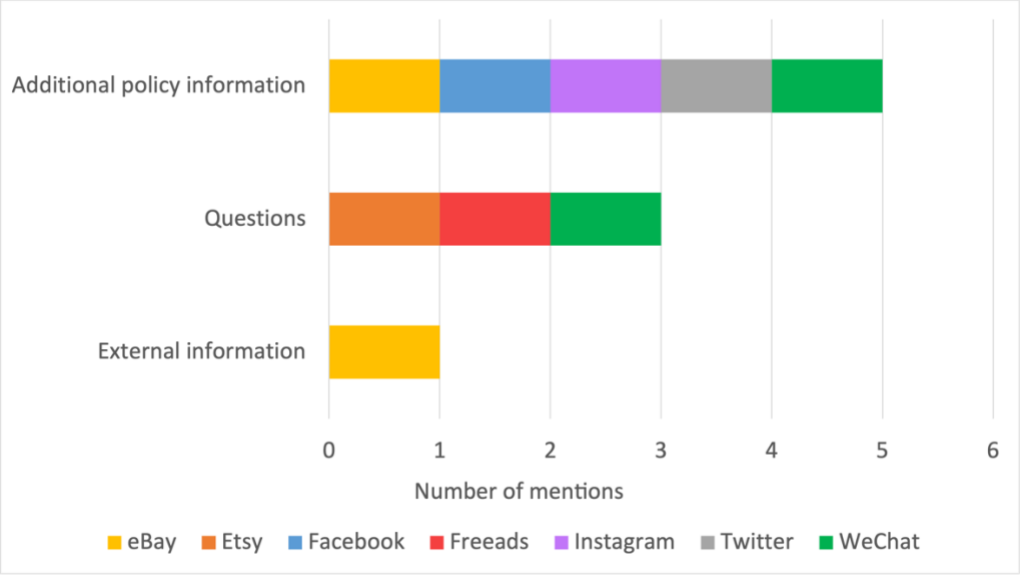


Figure 5.13: Number and kind of additional information provided in online platforms' illegal drug trade policies

56% of resources provided consisted of additional policy information including legal platforms' Terms of Service and specific enforcement policies and 33% consisted of links and email addresses to ask further questions. eBay also specifically referred to the Uniform Controlled Substances Act and provided a link to additional Food and Drug Administration resources about drug-related products to its users (eBay, 2020d). Overall, 56% of platforms provided only one type of additional information in their illegal drug trade policies and the remaining 44% were equally split between platforms which didn't provide any additional information and those which provided two types of resources.

Additionally, Facebook released two blog posts informing their users of their policies and efforts to disrupt illegal drug trade (Facebook, 2014, 2018b), as well as four bi-annual impact reports about their success policing drug sales on their site since May 2018, although only three are publicly available (Facebook, 2018a, 2019a, 2019b). As Instagram is owned by Facebook, one of the impact reports included that platform too (Facebook, 2019a). Their first

blog post mentioned the work they did alongside other government and non-profit organisations to update their policies and create educational resources aimed at their users (Facebook, 2014) and the second mentioned their involvement in the Tech Together to Fight the Opioid Crisis campaign (Facebook, 2018b). Their impact reports then provided additional information about the number of posts they detected and removed because they violated their regulated product policies, the number of posts reported by users, and the new techniques they have been developing and using to explain their increased detection rates (Facebook, 2019a, 2019b).

Legal platforms' illegal wildlife trade policies also differ from drug trade ones in this category.

All but two platforms provided additional wildlife-related links and resources to their users, though this information took different forms.

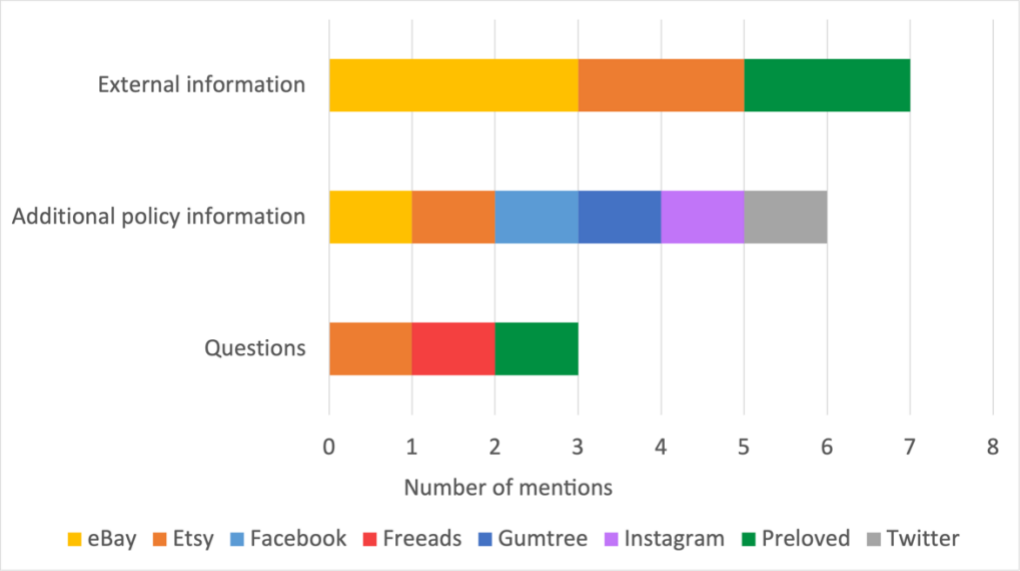


Figure 5.14: Number and kind of additional information provided in online platforms' illegal wildlife trade policies

While the distinct number of pieces of external information provided was the highest overall, additional policy information including Terms of Service and specific enforcement policies was included by the highest number of platforms – six. External information and opportunities for questions were then both included by three platforms. Of the former three platforms, Etsy and Preloved both included two links to external legislations about illegal wildlife trade, and eBay mentioned three. These resources included the "Convention on International Trade in

Endangered Species of Wild Fauna and Flora (CITES)" (1973), the "US Endangered Species Act" (1973), the "Wildlife and Countryside Act" (1981) and the "European Union Wildlife and Trade regulation" (1996). However, CITES' protection levels and the EU Wildlife and Trade regulation annexes were used interchangeably in the Preloved policy and additional posts. Overall, half of the platforms provided only one type of additional information in their policies, Pets4Homes and WhatsApp provided none, eBay and Preloved provided two, and Etsy provided all three.

Several legal platforms also released additional blog posts informing their users of their policies and efforts to disrupt illegal wildlife trade, as well as reporting on their successes. Of these platforms, Freeads posted animal checklists about birds and tortoises, among others, to encourage buyers to plan before adopting a pet (Freeads, 2019a, 2019b). However, these checklists were similar to the ones posted for cats and dogs and did not include any information about ensuring the legality of the animals for sale. Additionally, one of the most relevant checklists – exotic animals – was removed from the site since it was first accessed (Freeads, 2019b). Etsy and Instagram both released one blog post about protecting wildlife on their sites (Etsy, 2016; Instagram, 2017). Preloved released six blog posts, some explaining their ivory ban (Preloved, 2015b, 2015d), some providing more information about CITES and recent protected species updates (Preloved, 2017, 2020), and others providing caring guides for tortoises which included information about which breeds were legally protected and which weren't (Preloved, 2011, 2015c). Finally, eBay released eight blog posts about their ivory ban (eBay, 2008a, 2008b) and their efforts to combat illegal wildlife trade online alongside conservation organisations (eBay, 2016b, 2016c, 2017b, 2018b, 2019a, 2019b), as well as three annual impact reports about their successes in that fight, though all relying on similar information (eBay, 2016a, 2017a, 2018a). None of Facebook's community impact reports that mentioned progress in detecting and removing drug-related content made any reference to illegal wildlife species and products.

Overall, all but two legal platforms provided additional information to complement both their illegal drug and wildlife trade policies. Of those seven illegal drug and eight illegal wildlife trade policies, most platforms in both cases provided links to additional policy information on their websites and three platforms also provided a direct email address to ask further

questions. While only eBay provided a link to an external Food and Drug Administration resource as part of their illegal drug trade policy, the agency responsible for protecting public health by ensuring the safety of drugs (FDA, 2021), three platforms provided external links in their illegal wildlife trade policies. These three platforms also included more than one resource, Etsy and Preloved providing two, and eBay three. Overall, drug trade policies included nine pieces of additional information, two of which from group members, both referencing additional policies. However, overall wildlife trade group members included 11 pieces of additional information in their combined policies compared to five in non-members' policies. Additionally, group members included 83% of the additional policy pages and 70% of the external links, only lagging behind with 33% of the additional questions links. Only Facebook released additional blog posts related to their illegal drug trade policy and impact reports, while five platforms released blog posts, guides, and impact reports related to their illegal wildlife trade policies. This might therefore imply that there is more information to be communicated about illegal wildlife trade as rules and regulations vary across countries, but also that such policies might require more justification than drug policies do. Indeed, the latter might be more widely understood as being illegal than the former. However, these results are still limited given that TRAFFIC, WWF, and IFAW (2017) included nine different links to wildlife trade laws across regions and products for inclusion in legal platforms' individual policies.

Raising awareness and providing information about illegal trade were both widely advocated for by Police and specialised agencies (IFAW, 2014a; EMCDDA and Europol, 2017a; IFAW, 2018a; EMCDDA and Europol, 2019; Coalition to End Wildlife Trafficking Online, 2020), however many policies seem to be lacking on that front. While providing links to more precise policies and ways to ask for further information are helpful in educating users, external resources are seldom included when they would provide more thorough and official information. In both products' cases, links to relevant rules and regulations both locally, nationally, and internationally should be provided for users to peruse at their leisure and not have to seek out relevant legislation on their own.

Provided these trade policies are present and comprehensive on legal platforms, they could ultimately reduce illegal trade on these sites if they are complemented by monitoring, information sharing, direct intervention, and awareness raising.

5.2.2 Platform monitoring

Monitoring should not be a new activity for several legal platforms, as many have been monitoring other issues on their sites for years, so existing detection systems can be repurposed to monitor illegal trade (LP-W1).

Monitoring takes several forms for these platforms, from filters that scrutinise listings before they are posted so certain keywords do not appear on the sites (LP-W1), to automated machine learning systems that examine listings regularly after they have been posted in case any information evolved or some listings were let through to the site that shouldn't have been (LP-W1; LP-DW1). When listings are flagged through either process, they are then reviewed by a team specialised in these products, trained for this reviewing purpose, aware of the relevant legislations, and able to make informed decisions (LP-W1). The more the teams understand which types of illegal listings are let through, the more the platforms can refine their algorithms accordingly and ensure the number of these illegal listings declines over time (LP-W1). Algorithms can also be refined as new items are restricted or banned on specific platforms, or as new codewords are uncovered that refer to illegal products (LP-DW1).

This constant monitoring process ensures that most potentially illegal listings are flagged and not posted on the site. However, there are still instances when they do get posted (LP-DW1), as the sheer volume of content on these platforms makes it difficult to monitor, even through automation, allowing some criminals to sit in plain sight (POI-D4). The responsibility for letting these illegal listings be posted is that of legal platform administrators, which are often accused of not trying to stop illegal trade on their sites (LP-DW1, P-W2). However, despite great amounts of money and effort being put towards monitoring, some illegal products are always bound to filter through these systems (LP-DW1).

"Go to 2009, and IFAW and a couple of other organisations put a lot of pressure onto eBay to say 'you shouldn't be selling ivory, it's a problem'. eBay said 'well if it's illegal we'll just ban it' and so you can't sell ivory on eBay. But now the issue with that is that of course people just renamed it, so it's become 'ivory-coloured', 'bovine bone' or whatever they happen to call it at any one time and so although ivory is banned, there is probably at any one time about 1,000 items of ivory on eBay if you do a quick search." (P-W2)

Specialised organisations and individual users have therefore attempted to help.

5.2.3 Information receiving and sharing

Legal platforms are not only at a crucial place to share information with the Police following their monitoring activities, but also to receive information from other individuals and organisations performing their own monitoring.

As well as gathering their own information about their users and listings through monitoring, legal platforms often receive tips from organisations and individuals reporting unusual activity. Although one interviewee mentioned reaching out to these platforms and not being welcome in to support them (POI-W1), many organisations and individuals have. Several animal welfare organisations are also monitoring these platforms and flagging up potentially illegal content to their administrators, as will be detailed in the next chapter. Users also report listings on websites that contain illegal features or contact the sites' customer service teams to raise these issues (LP-W1). A legal platform administrator remarked that many of these active users were in fact users who were banned from the site for posting illegal listings themselves and now report their competition, so they are also removed from the site (LP-W1). This is similar to Krebs (2015)'s observation that spammers, persons or organisations who send irrelevant or unsolicited messages over the Internet, try to sabotage each other by sharing information about the other's practices. Upon receiving this information, they are then able to refine their monitoring systems so fewer illegal listings pass through them (LP-W1) and they possess even more information about their users in case it is required by the Police.

Some legal platforms have also described being in constant communication with the Police, as agencies are likely to contact them every day regarding several issues on their site, including tax or security as well as illegality (LP-W1). Under the new GDPR regulations, the Police need to be allowed to request certain information. Legal platforms can then share relevant data with them for their investigations, or more rarely provide support as part of these investigations (LP-W1). It is more unlikely for legal platforms to contact the Police, however, as much data, evidence, and time would be required to take cases forward (LP-W1).

> *"We would report people to law enforcement but it hasn't happened because we are not in the position to really make a claim there, we don't have enough evidence and data on the people. We can send them a message and say 'have a look into this one', but they want hard information, so that would be a constant ping pong communication between us and them and we just can't do it because it's too time-consuming." (LP-W1)*

In some cases, legal platforms have therefore encouraged individual users to report others to the Police, if they have a vested interest in bringing these cases forward and policing this kind of behaviour (LP-W1).

Such information receiving and sharing is vital to connecting policing groups around a pivotal point, legal platforms, and to forming a fuller picture before further action can be taken.

5.2.4 Content removing and User blocking

As seen in the legal platforms' trade policies, removing content and blocking users were common enforcement practices for users who failed to abide by the platforms' rules.

Interviewees therefore confirmed that they or their partners proceeded to removing a lot of listings and blocking several users and conversations (LP-W1; LP-DW1; POI-D6), as well as disabling users from creating platforms on sites which were not trade-focussed (POI-D6). However, these measures would only be taken if and when administrators knew for certain the products or services listed were illegal and vendors knowingly listed them anyway (LP-DW1). In some cases, administrators even reached out to each user individually to explain why certain listings were taken down or accounts blocked (LP-W1). As can be imagined, users

whose listings were removed were often unhappy about these decisions (LP-DW1), as they sometimes disagreed with the site's logic for doing so, but most of the contests were done in private, so the platform's public image was not impacted (LP-W1). However, the general public using these platforms legally reacts positively to these removals, as people want to keep these sites legitimate. Administrators therefore know they have their support in taking these actions (LP-W1).

> *"It's much more fun to be the good ones. We get a lot of positive feedback, maybe not from the people who place the ads, but from other people and the organisations we work with, it just feels great!" (LP-W1)*

While some platforms prefer not to disclose this information (LP-W1), some will report on the number of removals and blockings they performed (see the 5.2.5 Awareness raising section). When that is the case, it should be noted that upon calculating the amount of reported removals as a proportion of total listings, assuming the totality of illegal listings cannot be taken down, people questioned the veracity of legal platforms' content removal claims. Indeed, it was argued that the reported numbers would mean having more listings on these platforms than actually witnessed (POI-W1).

Removing content and blocking users on their sites is the sole direct intervention legal platforms can conduct in response to online illegal drug and wildlife trades. Legal platforms are therefore seen to possess certain powers and authority on their own platforms in order to ensure their security and that of their users. Not only can legal platforms report on their interventions, as the Police do, but they can also raise awareness about illegal trade issues more generally, which many have done through their sites.

5.2.5 Awareness raising

As well as publishing trade policies to regulate illegal activity on their sites, online platforms have also been instrumental in raising awareness about illegal trade issues to the wider public by publishing additional content in the form of blog posts and reports (LP-W1; LP-DW1; eBay, 2008a, 2016c, 2019b; Facebook, 2014, 2018b).

A big part of these platforms' awareness raising activity has been related to the evolution of public awareness about illegal trade. While a large part of the population remains unaware of these issues and needs educating, another part has become drastically more aware and legal platforms have had to respond to these societal changes (LP-DW1). An increase in awareness about illegal wildlife trade specifically began when animal welfare organisations pressured eBay to ban the trade of ivory on their site in 2007, although other smaller platforms at the time did not focus on these issues (LP-W1). Since then, more legal platforms have banned this trade and others to respond to public demand, and most of them explain their reasoning when such steps are taken (LP-W1; Preloved, 2015d). Part of this awareness raising also involves mentioning other related successes such as enforcement operations, for platforms which are large enough to develop their own regular content and keep their audiences engaged on these issues (LP-W1). However, while this constant and important work is happening in the background, legal platforms do not all report on their own performance in policing illegal trade on their site. Facebook is a good example of showing their audience how many posts in different categories have been caught by their detection mechanisms and how many by their users, showing evolutions over time (Facebook, 2018a, 2018b, 2019a, 2019b). Other organisations, although they mention seeing improvements in their detection mechanisms over the years, as fewer potentially illegal listings are let through to their site, are less forthcoming about these numbers and instead prefer to focus on the issue in broader terms (LP-W1). It should be noted that beyond proactively raising awareness and sharing this information, some platforms have also had to communicate about these issues more reactively, responding to unexpected "*hit pieces*" about the amount of illegal trade housed on their sites (LP-DW1).

As shown by the amount of blog posts and reports published by various legal platforms, raising awareness plays a big part in ensuring users understand what constitutes illegal trade, how they can legitimise their purchases if they sit in a grey area, and why ensuring the proper trade of these products is paramount for our health, environment, and security. Such awareness often takes the form of providing access to documentation and explanation for certain rules, as shown in legal platforms' provision of additional information as part of their trade policies. Reports of interventions performed by platform administrators and moderators can also participate in this education. Awareness raising is performed to preserve

platforms' legitimacy by ensuring users know what they can and cannot trade, to respond to allegations of housing illegal trades, and to support societal pressures that deem these issues worthy of further action.

The answer to our second research question is therefore that legal platforms police online illegal drug and wildlife trades on their sites by publishing trade policies, monitoring listings and their sites both manually and automatically, receiving and sharing information about criminal listings and users, removing illegal content and blocking the users who post them, and raising awareness about these trades and their interventions to reduce them.

The answer to our third research question is that these activities are the same when policing both online illegal drug and wildlife trades, although the policies initially published by legal platforms differ in their comprehensiveness between both products. All of these legal online platform activities are summarised alongside the activities conducted by the Police, private organisations and individuals, and cybercriminal traders in the policing script devised in the Discussion chapter.

Despite these slight differences between the policing of online illegal drug and wildlife trades performed by legal platforms, the ways these policing activities can be rendered more effective in the future are similar for both products.

5.3 The future of legal online platforms

Due to their prominent role in this type of policing, yet limited prior knowledge and resources to be able to deal with these illegal trades, legal platforms have depended on the Police and private actors for their policing activities.

The groups discussed throughout this chapter, including Tech Together to Fight the Opioid Crisis, the Center for Safe Internet Pharmacies, and the Coalition to End Wildlife Trafficking Online, have shown the importance of cross-sector collaboration when it comes to legal online platform policing. Indeed, although these sites have had processes in place to filter listings and collaborate with the Police and other agencies about other types of trades, the support they have received from these groups has been crucial.

> *"For us it is very helpful to work with external organisations because they have another view on things and also they have mostly deep knowledge we might not have in that moment in time. […] The best strategic decision we have made in that regard was to work with an organisation like [animal welfare organisation] because we did not have the deep knowledge inside our organisation, so they helped us a lot" (LP-W1)*

Legal platforms' continuous support and acceptance of any private actors who might be willing to help will therefore be paramount to addressing this challenge holistically. Specifically, it will be important for legal platforms to unify not only their policies, as done as part of the above groups, but also their interventions. Indeed, as theories of displacement have shown, if a trader is blocked from one platform or their content removed, it is likely they will migrate to another platform or create a new profile on their current platform. In order to prevent this, all online platforms should possess the ability to detect illegal content and then intervene in a similar way, so that traders do not have these options. It could be argued that trade would then relocate to another domain of activity altogether, such as the Darknet as is already the case for drugs, which might be more difficult to monitor and control.

It should be noted that these monitoring activities are first and foremost aimed at protecting the public from dangerous and illegal trades, but they also protect legal platforms' reputation in the eyes of the public. To ensure the protection of the public and the carrying of justice

take precedence over these capitalistic motives, private policing through these platforms should not be performed in a silo. Indeed, unlike the in-house private policing of physical organisations which is responsible for a limited number of people, the policing of these platforms impacts millions of users around the world. The Police should remain involved with their interventions, as their aim is the wider protection of society. By continuing to perform arrests following this monitoring and the detection of significant illegal activity, the Police will hopefully reduce the attractiveness of these trades and discourage traders from moving from one platform to another. However, this displacement would be the case if the only consequence of traders' criminal behaviour was the removal of their content and blocking from one or several platforms. As discussed earlier in this chapter, involving the Police would require a lot of time and effort on the part of legal platforms communicating relevant information with them. The Police would also need the time and resources to deal with these additional investigations and interventions. However, the impact these coordinated efforts would make on the ecosystem as detailed above should not be underestimated.

The answer to our fourth research question is therefore that increased collaborations between legal platforms and other policing actors in the public and private realms, for trade policies publishing, platform monitoring, information sharing, content removing, user blocking, and awareness raising, can further increase the effectiveness of online illegal drug and wildlife trades policing. These collaborations are at the centre of the policing script presented in the Discussion chapter, as it is argued understanding the goals and skills or other entities will spur further collaborative interventions in the future.

5.4 Conclusion

This chapter presented an exploratory study into the evolving role of legal online platforms and their contribution to the policing of the online illegal trades of drugs and wildlife through the use of expert interviews and the content analysis of their trade policies.

Beyond the Police which play a key role in the policing of illegal trade on the Darknet, legal online platforms participate in the policing of the online illegal trades of drugs and wildlife by publishing policies restricting these trades on their sites, monitoring their sites to identify illegal listings and users, sharing relevant information with the Police and others, removing illegal content and blocking criminal users, and raising awareness about these trades and their interventions.

This chapter was divided in three parts: the first part presented findings about the legal platforms involved in the policing of these trades; the second part then analysed the activities these platforms perform and how these differ between the policing of online illegal drug and wildlife trades; and the third part discussed how legal online platforms can be more effective in this type of policing in the future.

Illegal drug and wildlife trade policies on legal platforms exist on a continuum of comprehensiveness with regards to their length, content, language, enforcement and reporting mechanisms, and additional information provided. However, the policing activities performed by these platforms remain consistent whether they intervene on illegal drug or wildlife trades. The similarities in these policing activities likely stem from the voluntary support these platforms have received from private specialised organisations, which perform specific steps as part of this policing and encourage legal platforms to perform others they are most suited to, such as internal monitoring and illegal content removal. These private organisations and individuals are the subject of the next chapter.

6 Private Organisations and Individuals

Drugs and related products, now constitute two thirds of all traded products on Darknet markets (EMCDDA and Europol, 2017a). They are also increasingly traded on the surface web (Babb, 2014; Thanki and Frederick, 2016; EMCDDA and Europol, 2019; Moyle et al., 2019). While illegal wildlife species and products are not widely available the Darknet (Harrison et al., 2016; Cugniere et al., 2019; Wright, 2019), up to 80% of this online trade might now be happening on social media platforms (Krishnasamy and Stoner, 2016), freely and easily accessible by many across the world (IFAW, 2018a; WJC, 2018a; TRAFFIC, 2019), and therefore representing another enforcement challenge (Martin et al., 2018b).

Drug and wildlife products have been compared in the literature for their many similarities, but drugs are the product that has received the most attention related to its Internet-mediated trafficking (Lavorgna, 2014a), while wildlife species and products are just now starting to be referred to as a mild threat (Europol, 2017g) following years of lobbying from welfare organisations (South and Wyatt, 2011). Due to the Police's limited resources and capacity in the policing of online illegal trade, as well as legal online platforms' lack of expertise in these matters, there has been a need for other stakeholders to get involved. Actors external to the Police in the private, public, and non-profit sectors have therefore been investigating these crimes and participating in their policing. Indeed, academic, NGO, and government stakeholders have been helping to combat illegal wildlife trade in the UK (Moshier et al., 2019). NGOs specifically have been argued to take on three main roles to support the Police in their wildlife trade policing endeavours: 1) campaigning to raise public awareness, 2) enforcing relevant laws when they are not enforced by the Police, and 3) lobbying government organisations for further controls (Nurse, 2013). Specific organisations have been specialising in one or two of these roles (*Ibid*.). However, the above studies are limited in their scope. Indeed, Moshier et al. (2019)'s social network analysis of policing stakeholders focussed solely on the connections between these stakeholders and not the activities they perform. While Nurse (2013) details these activities, his work focusses on the role of NGOs, which are only one of the stakeholders involved in this type of policing. Additionally, neither study considered the online component of these trades or included drug trade, which represents a similar enforcement challenge. We therefore have much to gain

from researching both of these products as part of the same study, gathering complementary insights to provide useful strategies for their future individual policing. Such support actors and activities are therefore further investigated in this online illegal trade context.

The aim of this study is therefore to understand how private organisations and individuals contribute to this online policing to better situate this group in the cyber policing classification and policing script devised in the Discussion chapter.

Research for this chapter was conducted by analysing the content of 58 publications from CSIP, Cyjax, Flashpoint, IFAW, and WJC, and interviewing 12 experts in private industry, non-profits, and academia.

This chapter therefore focusses on private organisations and individuals while investigating this thesis' broad research questions:

1. Are private organisations and individuals involved in the policing of online illegal drug and wildlife trades?
2. What activities do private organisations and individuals perform?
3. How similar or different are the private organisation and individual actors and activities involved in the policing of online illegal drug and wildlife trades?
4. How can this type of policing be rendered more effective in the future?

In order to answer the aforementioned questions, this chapter is divided in three parts, each one focussing on different research questions. The first part presents findings about the private organisations and individuals involved in the policing of online illegal drug and wildlife trades; the second part then analyses the activities these private organisations and individuals perform and how these differ between the policing of online illegal drug and wildlife trades; and the third part discusses how private organisations and individuals can be more effective in this type of policing in the future.

6.1 Private organisation and individual actors

As identified by Moshier et al. (2019) with regards to illegal wildlife trade policing, researchers in government, non-profit organisations, and academia have participated in online disruption activities alongside the Police. Private organisations are also involved in the policing of online illegal drug trade.

Participants in the private sector, from technology conglomerates, to security organisations, and threat intelligence providers, emphasised that participating in the policing of Darknet markets, even if not directly related to their primary activity was "*the right thing to do*" and something that aligned with their ethics and values, as organisations with resources and research capabilities (POI-D2): "*we're the good guys and we want to do the right thing*" (POI-D1). Their involvement has therefore provided the Police with additional manpower when monitoring all the different Darknet markets now available (POI-D4).

Few non-profit organisations are involved in the policing of online illegal drug trade, as they do not possess enough resources to both gather and analyse data (POI-D3). However, some have been analysing data gathered by others (POI-D3). Although private organisations are not active in this trade area, several non-profit organisations aiming to protect the welfare of animals and/or bring wildlife traffickers to justice have joined in the fight against wildlife cybercrime by conducting their own investigations into cybercriminal traders and legal online platforms (POI-W2).

Additionally, academics whether on their own or in research groups are considered private individuals as they have specific knowledge and skills, conduct research, and share their findings with the academic community and relevant public and industry partners, which can include the Police if the case of suspicious activity (POI-W1).

> *"I will go on the Internet and I will look for illegal wildlife trade and ping it across to [the Police], because I know how they work. I will maybe find a seller with several items and send it to them and say 'ok here is a serious dealer' rather than sending them one off items. If there's a complicated legal aspect to it, I will explain why it's illegal, so I will not just say 'here is an illegal item' and let them guess why it's illegal, I will explain why I believe it's illegal." (POI-W1).*

Private organisations working in the fields of technology, finance, and transport are also private actors, as they possess expertise and resources in their domain and are sometimes sub-contracted to ensure security and enforcement in certain contexts where the Police would be less able to do so (POI-D6). Such organisations are not detailed further in this chapter, as no interviewees worked directly in these fields, so further research could be undertaken to provide an exhaustive list of private organisations and individuals in this arena.

Finally, individuals, groups, or organisations writing social media messages or blog posts about the state of the criminal ecosystem are also considered private actors, as they are supporting the Police in raising awareness about crime and security, which they do not always have the resources and know-how to do themselves (P-W3).

However, organisations associated with Customs or the United Nations, although they do not have the word 'Police' in their denomination, are Intergovernmental Organisations which possess enforcement powers such as seizing products crossing borders and participating in the writing of laws about various issues they specialise in. They were therefore included in the first empirical chapter. Legal platforms and their administrators and moderators are not included in this chapter either, as they are considered to be requisite policing actors in this context, rather than voluntary ones, as will be discussed later in this chapter. The previous Legal online platforms chapter was fully dedicated to their activities.

Additionally, these policing actors are distinguished from civic communities, voluntary associations set up to pursue a common goal or interest (Putnam et al., 1993) and "buffer communities from external, often global forces" (Tolbert, 2005). Indeed, while some groups such as the Coalition to End Wildlife Trafficking Online and the Centre for Safe Internet Pharmacies allow their members to perform activities together against these social and economic forces, other organisations and individuals act on their own and for their individual interest, therefore not benefitting from this social capital. Moreover, this concept has mostly been applied to institutions such as democracy in order to measure civic engagement, such as voting (Fennema and Tillie, 1999), and entrepreneurial (Tolbert, 2005) or religious institutions (Ying et al., 2014) to gauge communities' solidarity, tolerance, quality of life, and citizenry. Such social and economic structures can and hopefully will become paramount to

policing, as is starting to emerge through various groups forming to combat online criminal trade issues, but the trust they require, as shown later in this chapter, is not yet fully formed.

The answer to our first research question is therefore that private organisations and individuals are present in many sectors, shapes, and forms. These actors range from the largest technology conglomerates, to threat intelligence and conservation organisations, smaller non-profits and educators specialised in narrow aspects of this trade. Due to the interjurisdictional aspect of online trade, the involvement of all of these private organisations and individuals has been indispensable for the Police and legal online platforms in order to police these trades effectively. Private organisations and individuals are therefore the third part of the cyber policing classification devised in the Discussion chapter. The following section analyses the specific activities they perform as part of this policing.

6.2 Private organisation and individual activities

Insights from interviews and content analysis have highlighted four main activities performed by private organisations and individuals to disrupt online illegal drug and wildlife trades: 1) Information gathering, 2) Intelligence sharing, 3) Expertise provision, and 4) Awareness raising. These are analysed in turn and the specific activities involved in policing both products are emphasised where they differ.

6.2.1 Information gathering

Although private organisations and individuals cannot take the same actions as the Police, they can participate in the initial step of any operation: information gathering. The term 'information gathering' is employed here as private organisations and individuals are not investigating specific traders or products as the Police do, instead they just monitor legal platforms and gather relevant information.

> *"We're not an investigative body, we do not have the remit, we do not have the tools, we do not have the legal right to go and investigate crimes on our own. Equally, we don't have the ability to go out and seize things, this isn't our role, we're not law enforcement, we're not the legal system, we're not judges. We can play our part, we do have a lot of visibility of what's happening on the Internet, so we have a very wide breadth of understanding of what's happening in the threat landscape." (POI-D1)*

Across sectors and products, interviewees talked about how important monitoring Darknet markets and legal platforms was for them, allowing them to better understand the scope of the threat (POI-W4) as well as the next threats facing their clients (POI-D1, POI-D2, POI-D3, POI-D4, POI-D5). Indeed, the Police protect society in general, private organisations protect their customers by identifying what is new, significant, and potentially dangerous that they need to pay attention to (POI-D1). Non-profits protect their cause by gathering up-to-date information to inform future action (POI-W2, POI-W5), and academics advance knowledge more widely.

The amount of information gathering performed by these different entities depends mostly on their resources, with some teams assessing 60% of their time is spent monitoring Darknet markets for this purpose (POI-D2), while some entire teams are dedicated to this process full-time in other organisations (POI-D4). The information they gather is also largely dependent on their goals, from attributing specific threats to human identities (POI-D2) to running test-buys in legal platforms to figure out how many online pharmacies are only fronts for identity and financial theft (POI-D6; Sugiura et al, 2012). This information is usually gathered using automatic monitoring techniques, such as spider crawlers scraping data on all the webpages they visit (POI-D4, POI-D5). However, such scraping isn't allowed on specific platforms, as certain sites are built to prevent it (POI-D4) and social media often requires manual integration due to these barriers (POI-W6). In these cases, analysts spend short periods of time manually reviewing and assessing these platforms before deciding whether additional and continued manual monitoring is necessary (POI-D4). The Chinese branch of a conservation organisation therefore mentioned that they monitor two social media platforms and the 31 most prominent legal trading websites in the country on a monthly basis (POI-W2) and others noted they have "*several forums*" that were useful for them to monitor regularly (POI-D5). The challenge with such monitoring, is that it recently moved from a single main platform where most of the trading was taking place, AlphaBay, to 19 major Darknet markets between 2017 and 2020 (UNODC, 2021d), to legal trading websites, social media and instant messaging applications, and now also to Dark web forums, further expanding the scope of material to review (POI-D4).

> *"When I first started, that was back in the days of AlphaBay, it was great, you had essentially just one single platform, one marketplace where you had all your vendors and all your buyers sitting under one handy Onion URL, which I could jump in on and check every day […] But it is obviously a very different ballgame now given all the law enforcement actions that have taken place over recent years. Things have developed massively from having just one or two marketplaces whereas everyone is now scattered across different marketplaces and forums and instant messaging and spilling over into social media in some cases. […] It's forever a game of cat and mouse, just trying to keep up with the trend of where people are*

moving to, new sites as they pop up, and then make sure we're keeping up with the curve" (POI-D4)

Additionally, Dark web forums are structured differently than Darknet markets, focussing on communications between users rather than trade. More content is therefore likely to be present, not only due to the nature of discussions but also because it is believed users are purposefully more chatty to create more noise in these forums and render monitoring more complex (POI-D4). Other less resource-heavy organisations such as non-profits look through Darknet markets more passively, as information is given to them for analysis by other actors in the field, because they do not have the manpower to look for it themselves (POI-D3). As well as the rising volume of content, another monitoring challenge is the regular change in codewords used by traders to refer to various illegal products, drugs and wildlife included, which have been difficult to keep track of (POI-D6). New information gathering techniques are therefore being developed, not only involving new technologies such as Artificial Intelligence which could automate the process (POI-W5, POI-W6), but also involving volunteers to render this process cheaper and further-reaching (POI-W5).

This last strategy employed by the Coalition to End Wildlife Trafficking Online through the work of volunteer Cyber Spotters creates a system in which monitors do not possess knowledge as detailed as that of hired consultants working on such tasks for two or three months (POI-W5). However, it spreads initial monitoring more widely, which experts can then build upon. Indeed, in more complex and resource-intensive cases, monitors will not only passively observe trade and gather the relevant information, but also interact with the traders in order to benefit from more privileged access. For instance, threat intelligence organisations have understood that they needed analysts monitoring these markets full-time in order to develop and maintain online personas to infiltrate more private groups, which traders would come to recognise and trust, with a view of being invited into select groups for additional monitoring (POI-D2, POI-D4). In the case of the Chinese animal welfare non-profit branch, this means actively connecting with cybercriminal traders on the platforms they monitor, who unsuspectingly accept their friend requests, allowing them to monitor their movements and provide more thorough evidence for further investigations and operations.

> "*Social media users think we are just another trader, they will not block us*" *(POI-W2)*

Information gathering and monitoring even extends offline, where private shipping companies have been found to have more checks in place than the US postal department to ensure the safety and legality of the merchandise they are delivering at every step of the chain (POI-D6).

Although they do so for a different purpose, private organisations and individuals involved in the policing of both online illegal drug and wildlife trades therefore gather information on the Dark and surface webs. This activity is differentiated from community policing, where members of the public provide the Police with crime-relevant information in their local community (Fielding, 1995). Indeed, while these partnerships aim to solve problems of crime and disorder (Gooch and Williams, 2015), this community policing initiative dating back to the 1980s mostly involves resolving conflicts, helping victims, preventing accidents, and fighting the widespread fear of crime (Cordner, 2010). In fact, crime work only represents a negligible amount of work performed by community police officers, whose working time is dominated by preventative work (Brown and Iles, 1985). However, in the context of this thesis the relevant private organisations and individuals actively participate in the policing rather than the prevention of crime as part of community policing partnerships. As shown in the remainder of this chapter, these organisations and individuals also go much further than this initial information gathering step. While the themes of partnerships and community are therefore present in this type of policing, they do not equate to community policing but are instead much more active and disruptive partnerships in this case.

Additionally, it should be noted that these organisations focus on gathering insights from these platforms instead of trying to shut down private group chats where criminal dealings and communications might be happening, or arresting cybercriminals (POI-D6). Indeed, these sites are of more use to them live, so they can continue monitoring them (POI-D4). There is therefore a clear tension for this entity between passing along information that requires further action from the Police and legal platform administrators, and the need for them to continue monitoring these individuals and platforms for their work.

Private organisations and individuals then need to analyse this information and disseminate it accordingly so further disruptive action can be undertaken.

6.2.2 Intelligence sharing

The Internet is too broad for any one entity to monitor it alone, so private organisations and individuals are not only monitoring these different platforms for their own purposes but they are also sharing their intelligence with others in order to put different pieces of the overall puzzle together (POI-D4), within the limits of their national laws (POI-D1; P-D2). The Internet has no boundaries, so it is paramount different entities work together in order to combat this form of crime together (POI-D1; International Compliance Association, 2020) and find ways to disrupt this trade effectively (Cyjax, 2018c). In order for sharing to be effective, information first needs to be analysed, often by sorting similar data together and noticing patterns and shifts (POI-W6). A collective vision and quantification is not always possible, as is the case for groups involving companies in various industries because they gather and quantify data differently (POI-D6), but organisations gathering this information are often able to get a general sense for these patterns. These information flows then take different forms as intelligence is shared by private organisations and individuals to: 1) the Police, 2) other private organisations, 3) legal online platforms, and 4) the public. Communications with the public are in the order of awareness raising, which is discussed later in this chapter.

Private organisations and individuals first share information with the Police. Such exchanges can emanate from both sides, with the Police providing information to private organisations and asking them to look into specific issues and sites (POI-D2; POI-D3; POI-D5), and vice versa if private organisations or individuals have data about a specific cybercriminal or site they want to inform the Police about for further action (POI-D2; POI-D3). The Police can hire specific organisations, if they specialise in threat intelligence for instance, to gather and analyse data on specific topics or sites and share it back with them, subcontracting their efforts (POI-D4). Without fully hiring private companies, Police agencies have also worked with organisations for sting operations, such as the yearly Operation PANGEA, a global operation targeting the online sale of counterfeit and illicit medicines and medical devices coordinated by Interpol to raise awareness about the risks associated with buying medicines from unregulated websites (Interpol, 2020). As part of these stings, the Police have received

transactional, personal, and payment information from private organisations and individuals behind the scenes (POI-D6). Other organisations, without being directly hired, have been keeping open communication lines with their local Police, speaking to them on a weekly basis (POI-D2) and reporting offenders (POI-W2) or trade listings (POI-W5) to them when necessary. However, interviewees admitted to coming across too many criminal instances to refer to the Police and lacking the resources to be able to report everything they see (POI-D5). In this case, they created a prioritisation system whereby only serious offences affecting national security and terrorism would be reported (POI-D5).

> *"I think there is a question of resource, should I report everything I see on the internet to law enforcement? Frankly, they are not really set up to receive everything that we spot, so there's a practical side to it […] we could fill our days with just reporting the stuff we spot, but then we wouldn't have any time left to do our main job, which is to support our customers." (POI-D5)*

Beyond private industry and non-profit organisations, individual academics and private citizens are also encouraged to pass information on to the Police if they come across suspicious listings to support their investigations (POI-W1). Indeed, academic ethics committees have now ruled that passing information on was not a problem, but this realisation only came recently (POI-W1). The same, however is not always so simple for other organisations.

As well as sharing intelligence with the Police, private industry interviewees also recognised that they needed to rise above any business competition when dealing with these threats, as it is often the case that "*they have half the data, we have half the data*" (POI-D2). Such organisations therefore mentioned working with any other groups that share their values and objectives in order to combat these crimes (POI-D1). These groups can be in different countries than their own (POI-D3), as long as it is within the framework of the law (POI-D1). This is particularly insightful when multinational organisations possess several national branches, which can coordinate with others in the country, but also report any information to other branches (POI-W2). In the case of non-profits, collaborations have proved particularly fruitful as organisations share the same goals without competing against one another as private companies do. They have therefore found natural allies to work alongside (POI-W5).

As the direct controllers of their own platforms, intelligence has also been proactively shared with legal platform administrators for content removal and user blocking, when instances of illegal trading have been witnessed (POI-W2), which require action from administrators as is their legal responsibility (POI-W6).

> *"We write to platforms and say 'we have noticed this activity, this contradicts either your own policy or the national laws x or y'" (POI-W6)*

Such communications have also been undertaken with moderators of social media groups to help them keep legality within their community (POI-W6). Future plans are also in motion to extend communications to engage with sellers directly on these platforms, to indirectly share messaging around illegality, and potentially even to undermine trust between traders as long as it respects proportionality and does not create harm (POI-W6), a technique which will be discussed further in the Cybercriminal traders chapter.

As these information flows involve several entities, alongside individual communications, a number of meetings and conferences have been organised to bring the relevant organisations in the same location to meet and discuss. Interviewees were able to list many such occasions when they came together with other experts to discuss the issues at hand. The meetings mentioned ranged from multi-stakeholder meetings organised by Interpol (POI-W1); to Wildlife Crime Enforcers conferences in the UK bringing together 100-200 Police officers, border force agents, and investigators (POI-W1, POI-W4); the Conference of Parties, a "*big melting pot of people*" (POI-W3), organised by CITES every three years bringing together national government representatives, private sector, IGOs, NGOs, and other interested stakeholders (P-W1); and meetings with other industry partners (POI-D2; POI-D4) or with the Police (POI-D6), governments (POI-D4, POI-D6), policymakers, and think tanks (POI-D3). When these meetings involve various sectors, they allow attendees to bring in unique perspectives and understand those of others (POI-D3), as they engage in roundtable discussions that enable them to share what they have seen and learnt from their own standpoint (POI-D6). However, these types of meetings are still rare and something which disrupters should work on developing further (POI-D4). Some participants mentioned the cost of putting together such meetings and explained they are therefore not able to organise some themselves but strive to attend others', as they are generally very beneficial (POI-W2).

Information sharing between various entities is therefore performed for both products. Indeed, most interviewees mentioned the importance of collaborating with other entities and sectors in order to disrupt illegal drug and wildlife trades online – "*collaboration is what will win this war*" (POI-D5). For many this means sharing information with one another as they are aware they only know part of the story (POI-D2, POI-D4). The ways this information was shared varied between entities, from officially being hired by the Police to provide intelligence (POI-D4), to discussing issues with trusted colleagues in other organisations over email or the phone (POI-D2, POI-W2) or participating in multi-stakeholder meetings (POI-D3, POI-W1, POI-W4, POI-W5). However, initiatives such as the Coalition to End Wildlife Trafficking Online and the Center for Safe Internet Pharmacies give the impression that the policing of this trade is more joined up and collaborative than it actually is (POI-W3). Indeed, experts do not necessarily trust others in other fields, as they don't believe in their abilities or motivations for helping this fight and are weary that they might be using that information for their own financial gain or organisational growth (POI-W1, POI-W3). Work therefore remains to be done to allow different organisations to understand one another and see the benefit of each other's input, as will be discussed further in the last section of this chapter.

6.2.3 Expertise provision

As well as intelligence, private organisations and individuals have been sharing their knowledge and expertise with the Police and others. This expertise provision has mainly taken two forms: providing another perspective where multi-disciplinarity is required and providing training and building capacity where necessary. Such expertise is not only shared between private organisations and the Police but also among private actors themselves across various sectors and to legal platform administrators, nationally and internationally.

Experts in the online illegal trade field are relied upon for their training and capacity building. For instance, NGOs are often asked to present to and educate government staff about illegal wildlife trade (POI-W2) and illegal drug trade (POI-D6). They are also working closely with the Police and train Customs and Police officers to increase their capacity to combat wildlife cybercrime (POI-W2), as well as providing help in Customs inspections, prosecutions, and attending general calls alongside Police forces in order to ascertain the illegality of certain wildlife products and species (POI-W1).

> *"Not all law enforcement officers have a chance to know the specifics of illegal wildlife trade, so actually they are very happy to know what NGOs are doing because we are free, we can always give them our response very quickly, unlike the government, so we can provide lots of expert knowledge to them" (POI-W2)*

These trainings also often involve sharing the experiences of seasoned officers and the ways they have handled wildlife cybercrime cases so new officers can learn from them (POI-W2). Experts in different sectors are also tasked with monitoring platforms on the Dark and surface webs (POI-W2) and providing intelligence to policymakers ahead of specific legislation discussions (POI-W2, POI-W4, POI-W5) and to clients (POI-W4).

Training and capacity building was also developed for legal platforms specifically, as NGOs well-versed in the issues and the relevant legislation were able to inform these companies on what they should be looking for and how they should deal with any offenses on their platforms (POI-W5). For these specific relationships, non-profit regional offices have been responsible for reaching out to legal platform administrators in their own countries and creating and nurturing these bonds to help them improve their trading policies and detection mechanisms. This has involved informing them about relevant legislation and training them in the art of platform monitoring and illegal activity detection, as they have already done as part of their information gathering activities (POI-W5, POI-W6). For legal platform administrators getting this support in training and expertise has been qualified as the best strategic decision they ever made (LP-W1).

The priority of both of these training activities is sometimes set by private organisations and individuals themselves, as was the case for Coalition to End Wildlife Trafficking Online founders reaching out to legal platform administrators in order to provide their services (POI-W5). It can also often be set by funders who select objectives for specific projects (P-W1) or clients who have concerns about specific threats (POI-D4).

Although private organisations and individuals involved in the policing of online illegal drug trade recognised a need for multi-disciplinarity in their endeavour (POI-D1, POI-D2, POI-D3, POI-D4, POI-D5, POI-D6), this was not put into action as evidently as for the policing of online illegal wildlife trade. Indeed, the findings related to private actors' expertise provision

overwhelmingly relates to expertise about wildlife trade. This likely stems from the majority of private experts in this sample not possessing specific expertise in drug trade and its policing, except for a few specialised organisations providing education in this space. This is the first stage at which private actors in the illegal drug and wildlife realms do not perform the same activities. Indeed, in the case of drugs, expertise is likely contained within Police agencies, as many have focussed heavily on drugs, which private organisations and individuals are making up for in the wildlife realm.

Regardless of its extent, expertise provision is a key activity performed by private organisations and individuals in this policing. This activity is a novel addition to the duties Nurse (2013) argued were performed by NGOs in the wildlife trade policing space, namely campaigning, enforcement, and lobbying. Indeed, his model overlooks the fact that NGOs and several other private actors have specific expertise that they can share with others, such as providing training and development for Police agencies, government agencies, and legal platform administrators by sharing skills only experts on these topics possess. However, this expertise is not always gathered for a common purpose. Indeed, while Pink and White (2016) argue that networks should share a common purpose for their activities, the entities under investigation in this thesis, and the private actors in this chapter more narrowly, all have their own motivations for getting involved in parts of this policing. This means that connections between these entities are possible, as already shown, but that a network of disrupters in this case cannot be reduced to actors with similar purposes. Instead, these connections are made more loosely, and private organisations and individuals will continue to build their expertise with their clients and causes in mind, rather than for direct enforcement and security purposes. Their information and expertise are then shared more broadly with the public.

6.2.4 Awareness raising

According to Nurse (2013), external organisations such as non-profits often take the role of raising awareness about conservation issues in order to influence future legislation, as rightly expressed by some organisations as one of their main activities (POI-W5). Indeed, online illegal wildlife trade specifically has been described as "*a very unpublicised online harm*" (POI-W6). Some information, albeit more general, therefore needs to be shared beyond policing

actors to the general public. Just like the Police, private organisations and individuals have therefore been publishing reports, blog posts, and news articles about their discoveries in order to inform not only the Police, their clients, and policymakers, but also the wider public about these threats. Private industry often uses blogs to that effect in order to freely, quickly and effectively share their research findings with the wider community, including their customers, to prevent future threats (POI-D1, POI-D5). For some, these free updates have acted as a good commercial tool getting people interested in their company and providing them with good feedback on their offering (POI-D5). Other organisations produce reports, which go more in-depth into these issues and provide a thorough overview about the research they have conducted and the associated findings (POI-W5). However, some interviewees noted that not all information can be shared, as the results of certain monitoring and detection is only made available to trusted partners, so as not to give cybercriminal traders a blueprint to further illegal trading. Legal reasons sometimes also prevent organisations from publicly releasing information, even if they are confident it is correct (POI-W6).

From speaking to their clients, some threat intelligence researchers have found that vast amounts of people are unaware of what happens on the Dark web (POI-D4). Summarising this information in short and regular blog or social media posts is therefore a good way to keep them updated on current happenings (POI-D4). Additionally, many traders are often unaware of the law prohibiting the trade of certain products, as restrictions about illegal drugs and wildlife often differ between jurisdictions. Indeed, Police agents themselves have realised they did not know some types of orchids could be illegal, for instance, so how could consumers be expected to know (POI-W1)? Certain countries have therefore taken the need to raise awareness about online illegal wildlife trade very seriously. For instance, China is showing videos to passengers landing in or departing from Chinese airports to explain the illegal aspect of these trades and what they are or are not allowed to carry with them, "*it's literally everywhere*" (POI-W2). Although the country banned the domestic trade of ivory, the product could still be found online. Additional Internet-specific awareness raising work was therefore performed by NGOs alongside legal platform administrators to avoid buyers assuming they would not be punished for buying wildlife products and species in this way (POI-W2). This included pop up alerts on trading websites and social media platforms if buyers were looking for certain keywords related to illegal wildlife trade (POI-W2, POI-W5). Other

organisations undertook research about audiences' responsiveness to various types of messaging, and found that people were more responsive to drug-related messaging around identify fraud and financial security, than messaging around health (POI-D6). The delivery of the content, as well as its core messaging, was also found to have an influence in the trust audiences put in it, as a drug education platform localised its message and partnered with community brands people were more likely to know and trust (POI-D6). However, awareness raising will only get rid of part of the problem: law-abiding-citizens newly educated about the issue. Other traders with criminal intent, even if they are aware of the rules will keep trading these illegal products (POI-W1). Additional policing operations need to be conducted in order to stop them. These operations have also been reported on in order to inform other policing entities and the public about efforts in the field.

Due to the differences in operations performed and the ways reporting organisations mentioned them, this final section will be divided between drugs and wildlife in order to show more relevant findings.

Throughout the 30 analysed private organisation drug-related documents, 218 references were made to 14 different policing operations. Market takedowns were the operations referenced the most with 53 mentions, and user blocking, network dismantlement, and honeypots the ones mentioned the least with only two references each. The other 10 operations were mentioned between five and 29 times. It should be noted that slander and Sybil operations were not mentioned in any of the analysed publications, confirming Police insights that these operations are not openly deployed (P-D2). However, one interviewee mentioned that Darknet market participants have become less trusting, making slander and Sybil operations prime disruption methods to exacerbate this erosion in communications (POI-D2), which will be discussed in the Cybercriminal traders chapter.

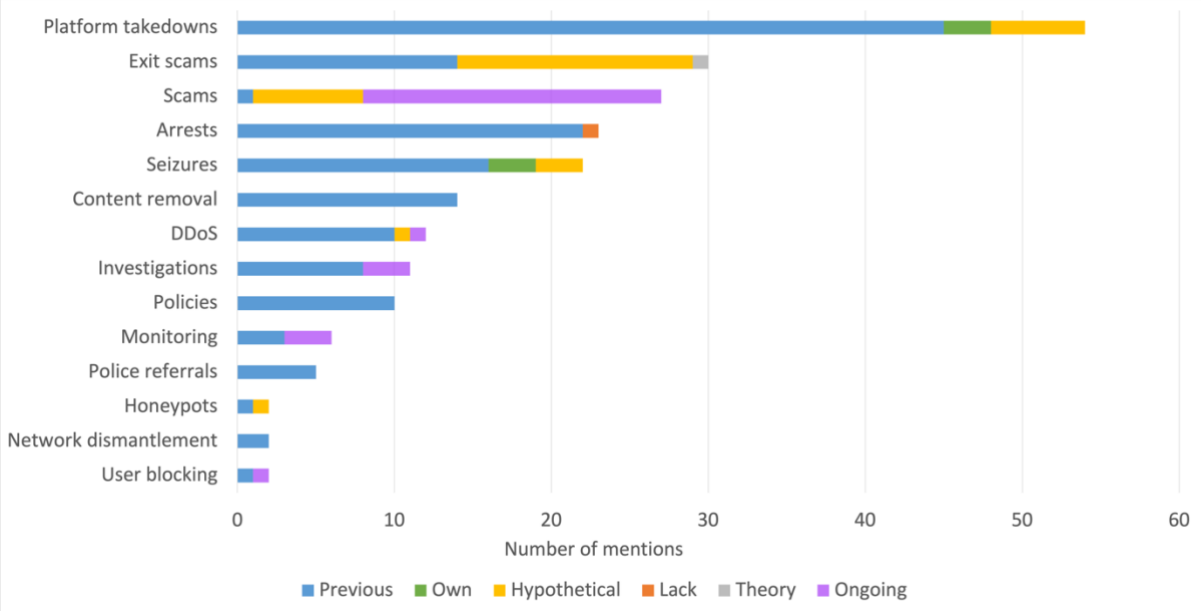


Figure 6.1: Overall number and types of mentions of different illegal drug trade policing operations

While gathering which types of operations are mentioned in these documents is important to understand what private organisations talk about in their communications, this chapter focusses on the *ways* these operations are mentioned. Further details about the six different types of references mentioned in private organisations' written public communications about online illegal drug trade policing are provided below.

With 150 mentions, or just over 68% of total references, previous operations were the ones mentioned the most across documents. This reference type is likely the one that is the most understood and expected in such documents, explaining to readers which operations have previously been performed, when, by whom, who was targeted, why, and any additional details writers decided to include. This reference type encompassed 14 policing operations.

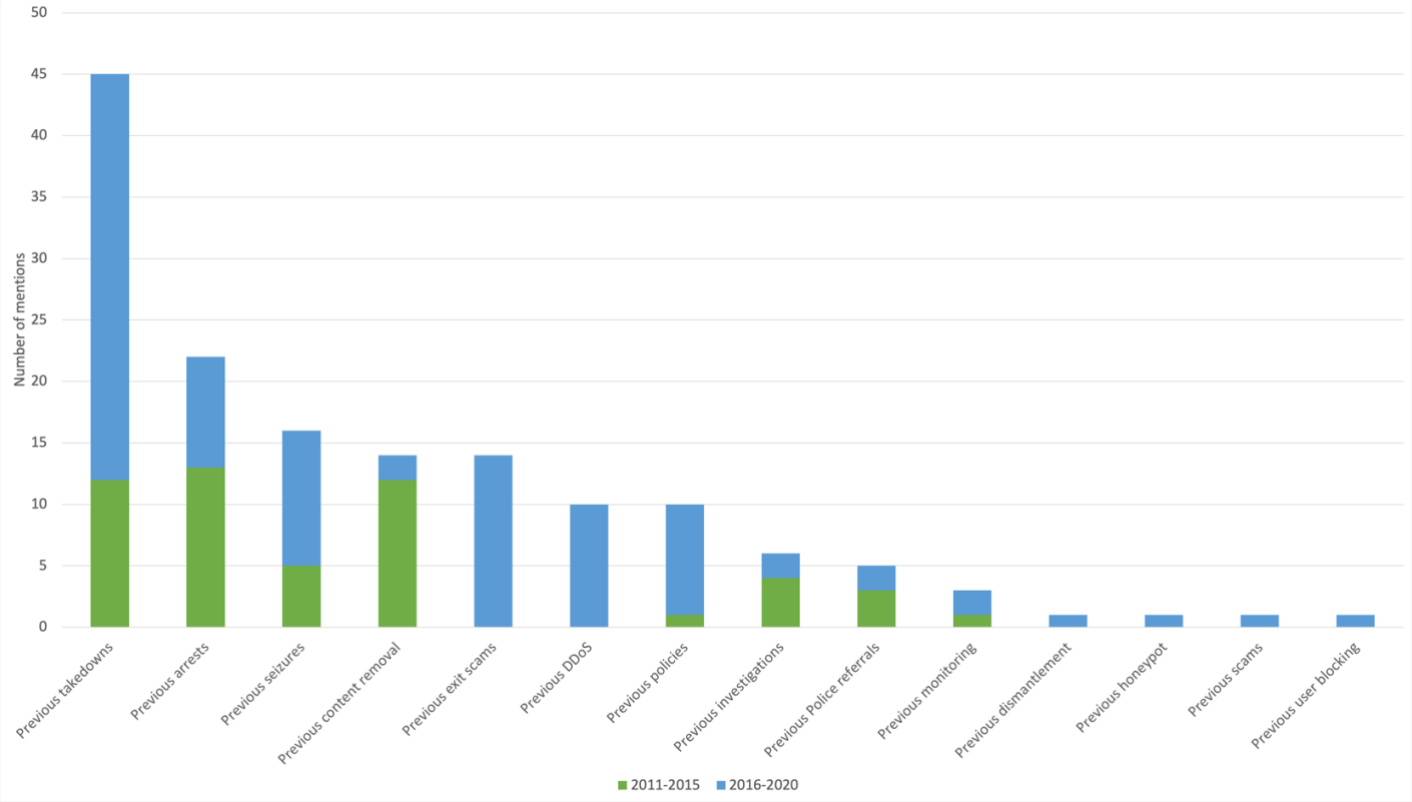


Figure 6.2: Overall number of mentions of different previous illegal drug trade policing operations over time

In some publications, these references only mentioned websites had been taken down (CSIP, 2012, 2013a, 2013c, 2013d, 2014a, 2014b, 2014c, 2014d, 2014e, 2016a, 2017), vendors, administrators or traffickers had been arrested (CSIP, 2012, 2013a, 2013d, 2014b, 2014c, 2014d, 2014e, 2016a, 2017; Cyjax, 2018a; Flashpoint, 2018b, 2019b) and products had been seized (CSIP, 2012, 2014b, 2014c, 2014d, 2016a, 2017). Less frequently, it was also reported that some administrators had exit scammed and left the ecosystem weakened and distrustful following their exit (Cyjax, 2018a, 2018b, 2020d; Flashpoint, 2016), that traffickers sold fake drug products (CSIP, 2014e), that private organisations and legal platforms had monitored various platforms (CSIP, 2013b, 2016b, 2018), and that some users had been investigated in

order to be held accountable for their actions (CSIP, 2013a, 2014b, 2014d, 2016a; Flashpoint, 2016, 2019b, 2020), sometimes as part of a whole network (CSIP, 2014b).

In other publications, precise names for the products that had been seized as well countries and timeframes for these seizures were given (Flashpoint, 2017a, 2018a, 2018b), as well as the names of specific marketplaces that were taken down, primarily AlphaBay and Hansa (Cyjax, 2017, 2018a, 2018b, 2020d; Flashpoint, 2017a, 2017b, 2018a, 2018b, 2019b), explaining how the Police gathered information as part of the month-long Hansa honeypot before the market was shut down (Cyjax, 2017). Certain publications also mentioned specific marketplaces that suffered from Denial of Service attacks during certain periods and the consequences these attacks have had on these marketplaces (Cyjax, 2018a, 2018b, 2020d).

In the case of CSIP which works closely with various private industry partners, their past accomplishments were also explicitly named. Indeed, they explained that sites such as Google and Microsoft had removed illegal content, mainly fraudulent advertisements for illegal online pharmacies (CSIP, 2013b, 2013c, 2014b, 2014d, 2016c, 2017), that they had blocked merchants (CSIP, 2016a), referred others to the Police (CSIP, 2013b, 2013c, 2014a, 2016b, 2016c), and updated their policies to ensure certain types of listings and content weren't let through (CSIP, 2013b, 2016b, 2016c, 2018).

The previous operations highlighted in these publications therefore did not only relate to Police interventions but also to private ones when the reporters had access to this information.

There were 33 references to hypothetical operations, just over 15% of total mentions.

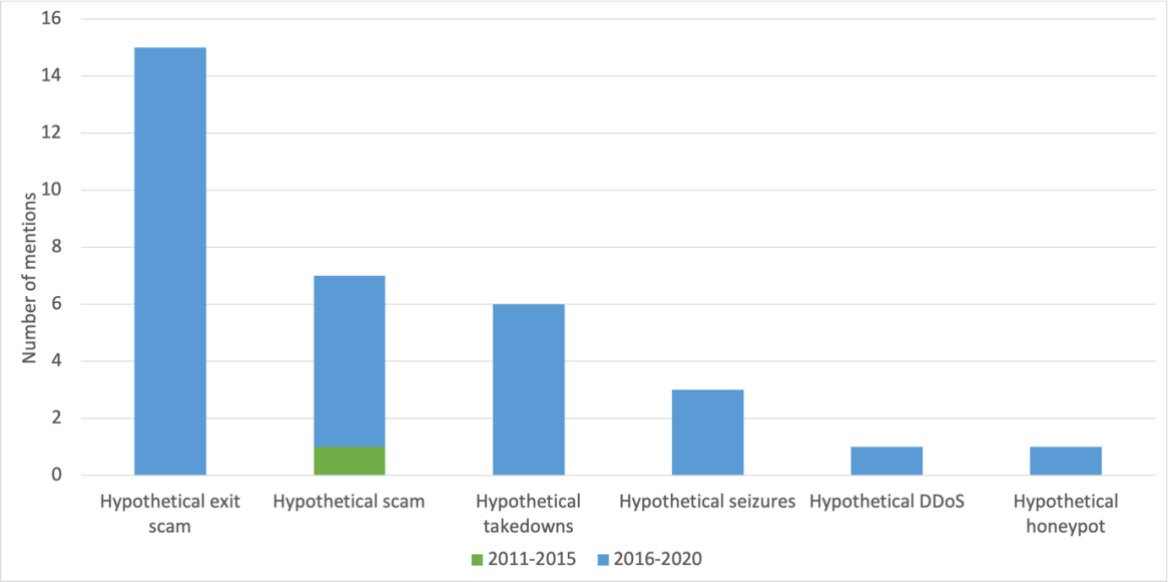


Figure 6.3: Overall number of mentions of different hypothetical illegal drug trade policing operations over time

Hypothetical mentions include unconfirmed past scams when no products were sent following purchase or counterfeit and dangerous products were sent (CSIP, 2013d; Cyjax, 2018a, 2018b, 2020c), and exit scams when administrators closed down their marketplaces and left with the money held in escrow (Cyjax, 2018a; Flashpoint, 2019b). This category also refers to future potential operations, such as taking down marketplaces in order to keep weakening the ecosystem (Cyjax, 2017, Flashpoint, 2018a), a likely risk of seizures if transactions involve transnational shipping (Flashpoint, 2017a, Cyjax, 2020c), the possibility the Police might perform a Denial of Service attack on Recon, a search engine including Darknet markets and the products they trade (Cyjax, 2020d), and the hypothetical rising distrust between users if they expect the Police to run other marketplaces like honeypots (Cyjax, 2020d).

Drug-related publications also made 27 references to five ongoing policing operations, several related to the coronavirus pandemic, just over 12% of total mentions.

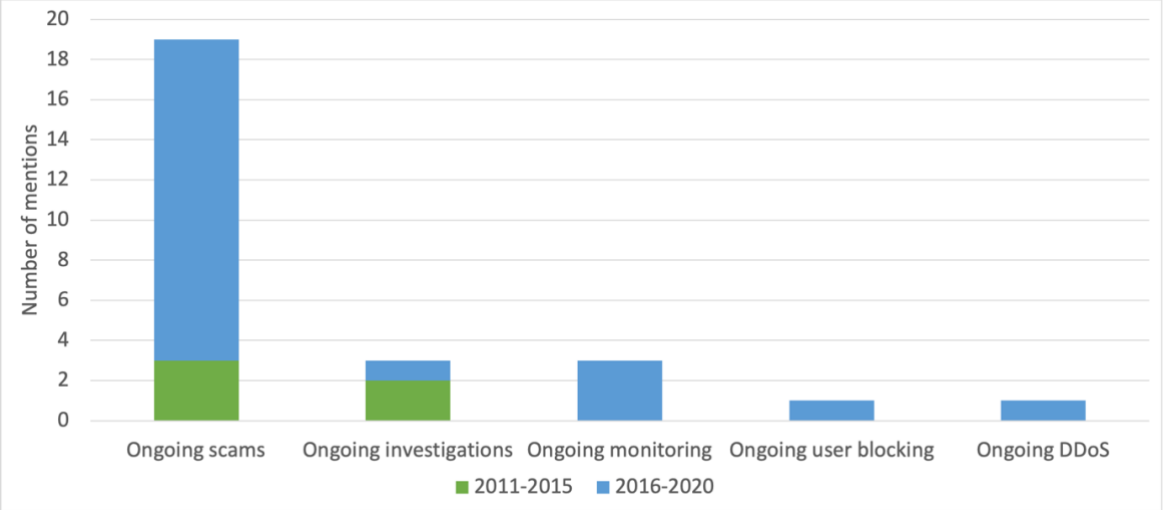


Figure 6.4: Overall number of mentions of different ongoing illegal drug trade policing operations over time

As shown by the other ways operations have been mentioned in private organisations' posts and reports, ongoing interventions are not expected as part of their communications, as they would signal to cybercriminal traders what enforcement action is underway on these marketplaces. However, when it comes to drugs, there is a real risk that listings for drugs or medicines are counterfeits and dangerous scams, therefore putting buyers at risk (CSIP, 2012, 2014c, 2014e, 2018). CSIP consistently reminds its readers about this threat, as well as reporting when previous interventions such as website takedowns and seizures have led to current investigations into scammers of interest (CSIP, 2014b, 2014d, 2017). Most recently, the centre also emphasised the monitoring being conducted on these marketplaces, and specifically that performed on social media platforms where large amounts of publicly available posts and keywords are available to track and report on (CSIP, 2020b).

Additionally, the recent pandemic has had an impact on Darknet trading. The vendors involved are now small, regional, and less-established, as larger vendors struggled with international supply chains when transport was restricted and delays were experienced through postal services. The types of products traded also evolved, as counterfeit medicines claimed to cure coronavirus surfaced in even larger volumes than usual (CSIP, 2020a; Cyjax, 2020c). Private organisations therefore worked to protect not only their clients but also the

general public about these risks, by explaining the interventions currently performed on these marketplaces. These interventions ranged from Police seizures to legal online platform administrators banning vendors and removing counterfeit listings, and cybercriminal traders themselves using this opportunity to scam buyers for their own financial gain (Cyjax, 2020c). Readers, non-malicious cybercriminal buyers included, could therefore get a better understanding of the risks involved on these marketplaces. CSIP also encouraged the public to report any listings they came across that claimed to cure or prevent COVID-19 infections, explaining the dangerous or even fatal consequences taking such fake medications could have (CSIP, 2020a)

Operations that the reporting organisations were directly involved in were mentioned six times in the analysed publications, just under 3% of mentions, all stemming from CSIP blog posts.

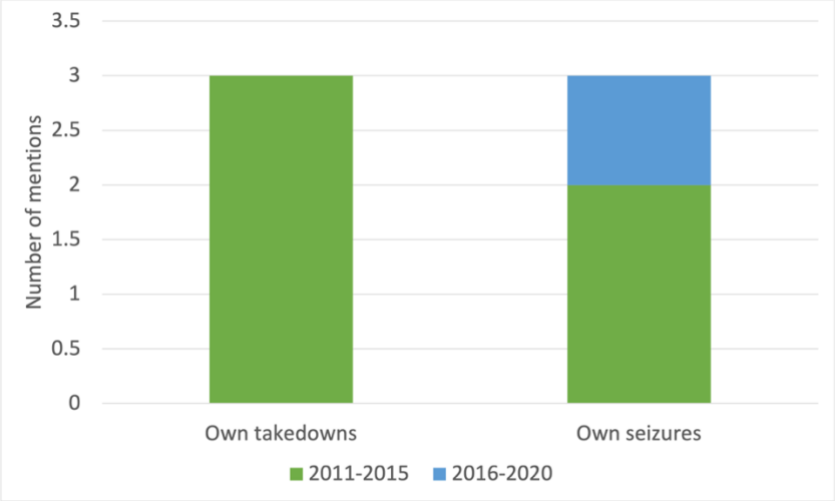


Figure 6.5: Overall number of mentions of different own illegal drug trade policing operations over time

Although Cyjax and Flashpoint did not reveal their involvement in enforcement operations in any of their publications, CSIP is a non-profit organisation relying on funding and aiming to raise awareness among its members about the work it is doing and the dangers of buying counterfeit drugs online. The organisation therefore reported on six interventions it took part in – three mentions relating to takedowns, several dozens of them undertaken simultaneously

each time (CSIP, 2013b, 2014c) and another three mentions relating to seizures, as the centre supported the tracking and interception of several tons of drugs in transit (CSIP, 2013b, 2014d, 2016a). Overall, and unlike other types of mentions in these publications, mentions of own operations decreased throughout the reporting period. It should be noted that these references were made in relation to CSIP as a whole being a participant in these interventions. Several additional blog posts pointed to the interventions their industry partners led, including Google, Microsoft, and Mastercard, which are counted as previous operations earlier in this section.

In the analysed documents, there was only one reference to a lack of arrests, therefore not increasing the perceived risk of using these marketplaces which would encourage traders to stop their activities (Flashpoint, 2019b).

Finally, there was also one reference to exit scam theory, explaining why vendors or administrators might be tempted to exit the Darknet ecosystem before the Police catch and arrest them or shut their marketplace down (Cyjax, 2020d).

The policing operations, the nature of their mentions, and their numbers differ in the context of wildlife.

Throughout the 28 analysed private organisation wildlife-related documents, 591 references were made to five different policing operations. Seizures were the operations referenced the most with 464 mentions, and network disruption the one mentioned the least with only seven references. The other three operations were mentioned between 11 and 62 times. An analysis of the timings of these mentions is not necessarily insightful here, as most documents were published from 2016 onwards, therefore skewing the results compared to earlier years. However, it was noted that similar numbers of operations were mentioned between 2004 and 2010 and between 2011 and 2015, 116 and 110 respectively, before this sharp increase.

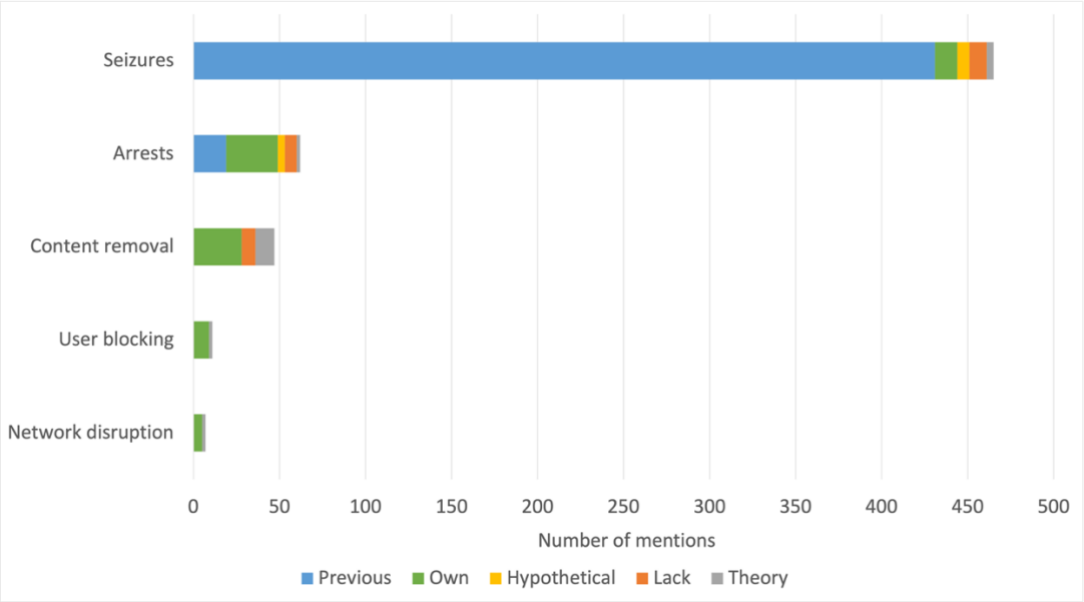


Figure 6.6: Overall number and types of mentions of different illegal wildlife trade policing operations

Further details about the five different types of references mentioned in private organisations' public written communications about online illegal wildlife trade policing are provided below.

With 450 mentions, or just under 79% of total references, previous operations were the ones mentioned the most across documents.

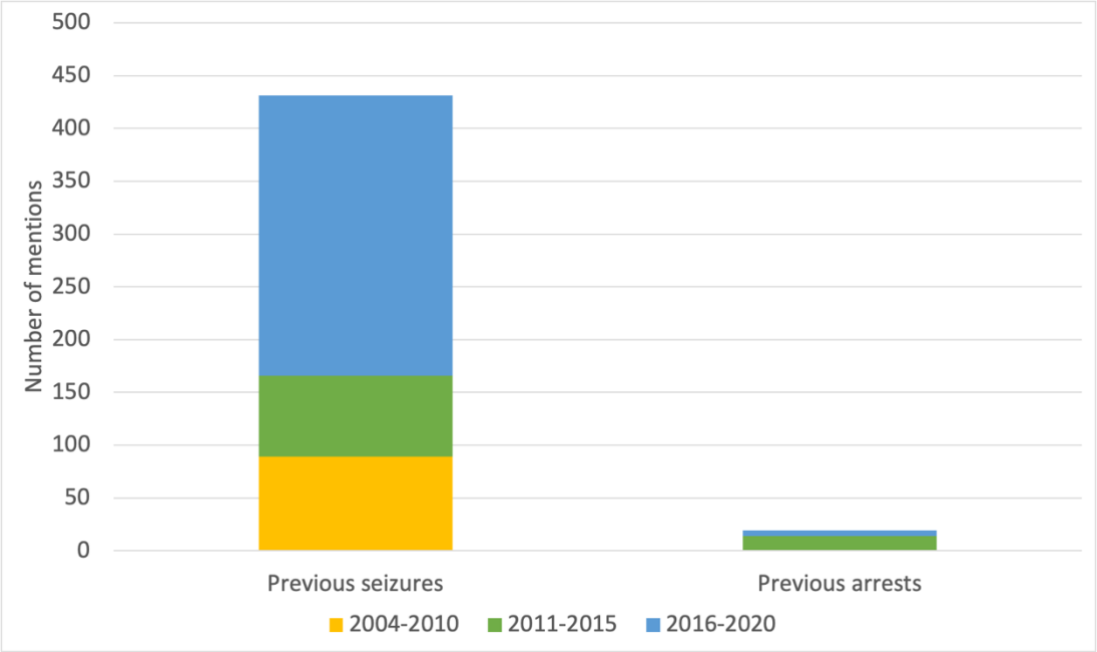


Figure 6.7: Overall number of mentions of different previous illegal wildlife trade policing operations over time

Sometimes, these references only mentioned seizures or arrests had happened in larger numbers than usual (IFAW, 2005, 2012, 2013, 2017a; WJC, 2017a, 2020c). Other times, precise names for the products that had been seized as well countries and timeframes for these seizures were given (IFAW, 2004, 2005, 2007, 2008a, 2008b, 2011, 2012, 2013, 2014a, 2014b, 2014d, 2017a, 2018a). These details are not necessarily relevant here, as this type of communication is expected in these kinds of publications. The other communication types below therefore require more attention.

With 85 mentions, or just over 14% of total references, own operations are the second most used reference type, relating to operations the reporting organisations directly took part in on their own or alongside others.

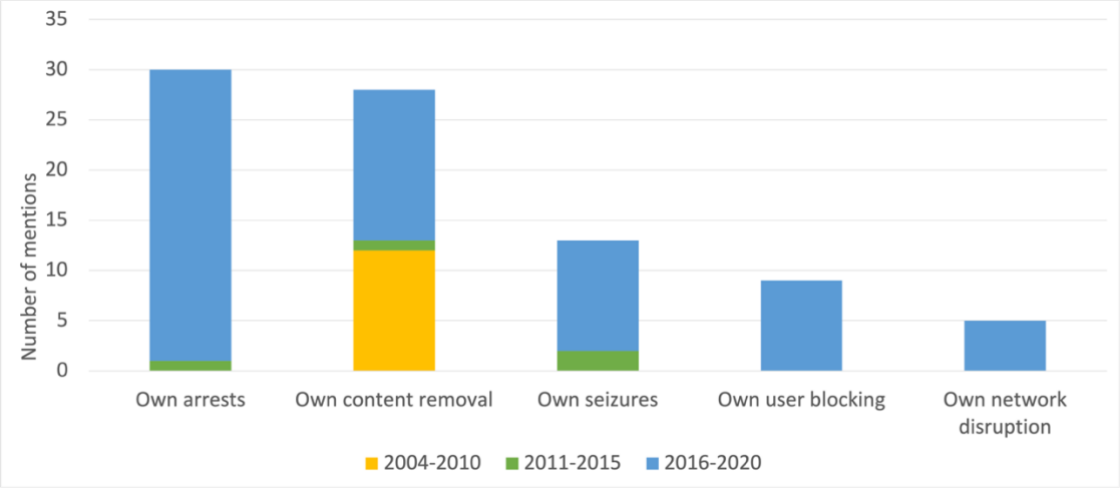


Figure 6.8: Overall number of mentions of different own illegal wildlife trade policing operations over time

Wildlife-related non-profit organisations spoke about operations they took part in, including arrests (IFAW, 2013; Coalition to End Wildlife Trafficking Online, 2020), seizures (IFAW, 2013, 2014b; WJC, 2016b, 2016c, 2017b, 2020c; Coalition to End Wildlife Trafficking Online, 2020), content removals (IFAW, 2005, 2007, 2008b, 2014c, 2014d, 2018a; Coalition to End Wildlife Trafficking Online, 2020), user blockings (IFAW, 2018a; Coalition to End Wildlife Trafficking Online, 2020), and network disruption (WJC, 2018a, Coalition to End Wildlife Trafficking Online, 2020). Although these references to operations following private organisations and individuals' support were often mentioned in general terms, some reports went into detail into the type of suspicious advertisements removed on a legal platform following reporting (IFAW, 2005, 2007, 2008b), or the number of persons of interest arrested, the enforcement agency which performed the arrests, and the location of these arrests following their input (WJC, 2016b, 2016c, 2017b, 2018a, 2018c, 2020c). It appears private organisations, for lack of being able to perform other tasks at the time, initially focussed on signposting illegal content to legal platforms which were then removed (IFAW, 2005, 2007, 2008b), before assisting with other policing operations.

There were 25 references to a lack of operations, just over 4% of total mentions.

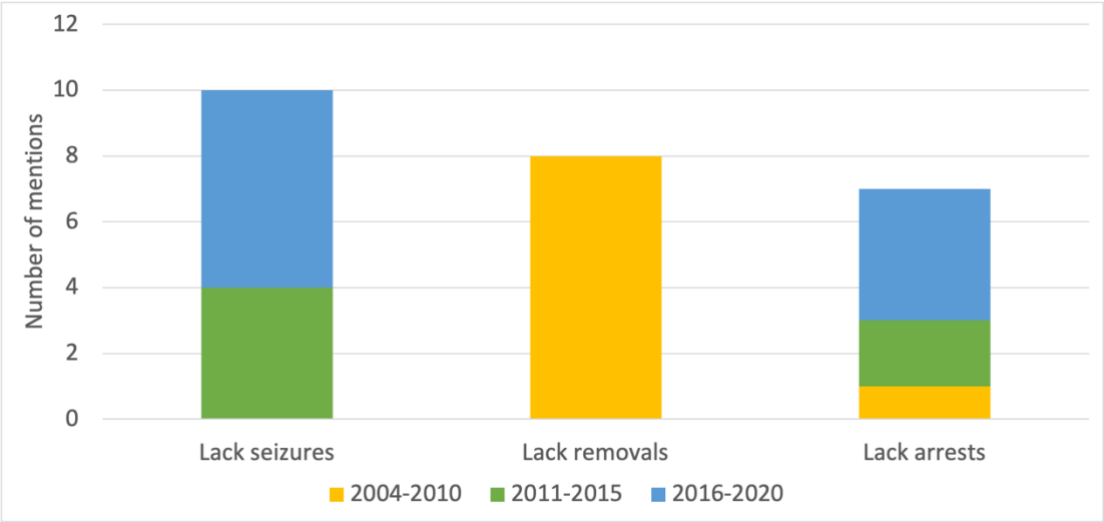


Figure 6.9: Overall number of mentions of lack of different illegal wildlife trade policing operations over time

A lack of arrests was mentioned (IFAW, 2005, 2013), including the specific inaction of the Vietnamese government only arresting one person when an entire file of persons of interest trafficking illegal wildlife in the country was shared with them (WJC, 2016b, 2017b). Seizures in specific locations and for specific products were also assessed as lacking when compared to other countries and forces with higher seizure rates (IFAW, 2013, 2014d; WJC, 2016c, 2018a, 2018c, 2020c). Finally, a few documents reported legal platform administrators' inaction and potential apathy in light of illegal trading on their sites, as very little content was being taken down despite reports about suspicious activity (IFAW, 2004, 2005 2007). They therefore advocated for the removal of any content that did not abide by platforms' trade policies (IFAW, 2007, 2008b, 2011, 2012, 2018a, 2018b), in order to remedy the issues they identified. These assessments were only made at the beginning of the analysis period (IFAW, 2004, 2005, 2007) and legal platform administrators seem to have become more responsive since.

There were 21 references to the theory behind operations, 3.5% of total mentions.

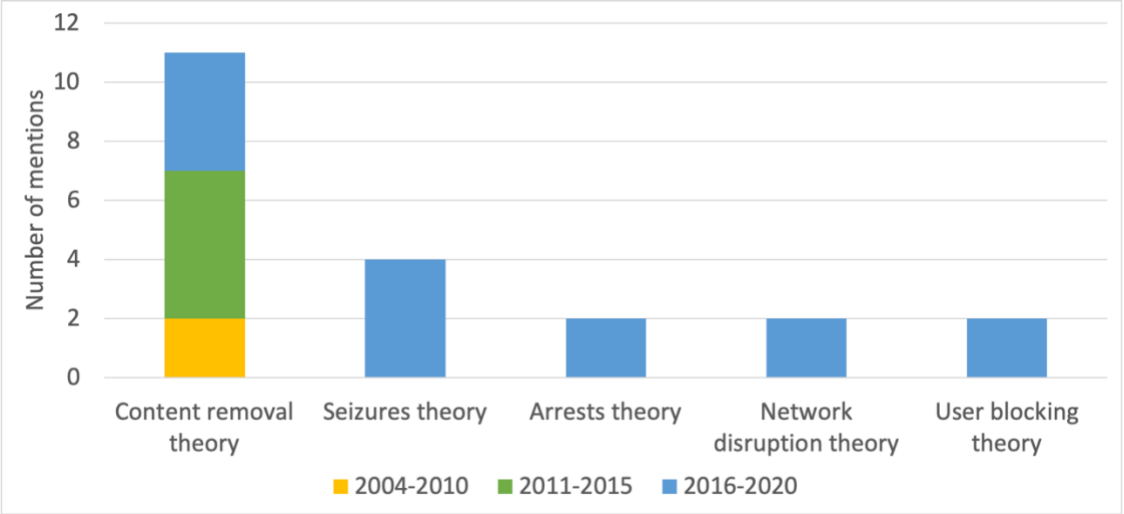


Figure 6.10: Overall number of mentions of different illegal wildlife trade policing operation theory overtime

Five operations were explained in more detail as authors aimed to justify why these operations might be conducted or why they might be performed in certain ways. For instance, certain reports explained why the most significant players are the ones targeted for arrests in each network (WJC, 2020c); what strategies might or might not disrupt networks effectively (WJC, 2018a); why seizures are needed in order to understand the products that are illegally traded and how they are smuggled (WJC, 2018a, 2020c); how much and how quickly various legal platform administrators are supposed to remove suspicious listings reported to them (IFAW, 2007, 2008, 2011, 2012, 2014c, 2018a, 2018b); and how Artificial Intelligence could help to block users posting such illegal listings more quickly (Coalition to End Wildlife Trafficking Online, 2020).

Overall, the number of theoretical references have increased over time, showing the complexity of the ecosystem and the need for the public to understand, at least in part, the actions of disrupters in this arena.

There were 11 references to hypothetical operations, just under 2% of total mentions.

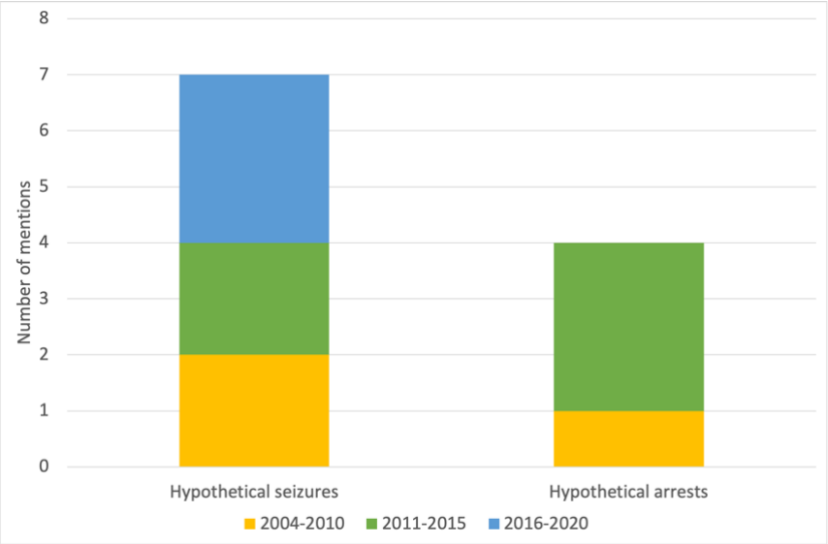


Figure 6.11: Overall number of mentions of different hypothetical illegal wildlife trade policing operations over time

In the case of wildlife, hypothetical mentions only relate to past unconfirmed operations, such as the possibility that arrests were performed (IFAW, 2004, 2013, 2014d), and unconfirmed seizures (IFAW, 2004, 2013, 2017a, 2017b), including cases in which corrupt officials might have hypothetically seized stock and only offered to release them in exchange for money. No hypotheses were provided about future operations as was the case for drug trade.

Overall, the number of hypothetical references have increased, not only conveying uncertain conditions in the ecosystem, but also an increase in the operations used to disrupt it.

Ensuring the public is informed about various issues pertaining to online illegal drug and wildlife trades is therefore an important part of private organisations' activities. The provision of information in news articles, reports, and blog posts often serves to inform cybercriminal traders and others about recent policing activities and to deter them from continued involvement in these crimes, as the perceived risk of identification and punishment is seen to increase. Unlike Police agencies, however, a general trend across interviews was that participants and their organisations did not want to reveal too much of their involvement in the policing of online illegal trade, so as to keep their research and investigations as covert as possible (POI-D4). While this was mostly the case of organisations raising awareness about online illegal drug trade, for which the number of publications and policing operation mentions were much lower than their wildlife counterparts, other organisations were more vocal. This is more likely the case for non-profit organisations which rely on external funding and therefore need to show potential funders the work they have performed (POI-D3). Such information has included the investigations they conducted, evidence they gathered, and results they obtained. It can be argued that cybercriminal traders expect the Police and others to be monitoring these sites, but they might not be aware of how many organisations or investigators are part of that effort, for which periods of time, and the specific products, users, or information they are monitoring. The danger with revealing too much of this information in blog posts and reports is that, unlike Police news articles about successful operations, private organisations' involvement might be less well-understood, and access to such reports might therefore shed some light on their strategies and alert cybercriminal traders to certain things they should do differently. This is precisely what private organisations want to avoid, as the longer illegal marketplaces are kept running and criminals are not too attentive to their presence, the more they can gather and analyse information (POI-D4). A balance therefore needs to be struck between information that should or shouldn't be shared. Partnerships could also be created, such as the ones described where private organisations share data with non-profits (POI-W3), where funding could be exchanged for analyses or other services, in order to render less apparent the work of private organisations in this policing.

A chronological analysis of different operations mentioned by private organisations shows that the ways in which these operations are discussed differ between illegal drugs and wildlife trades, as they are performed in different parts of the web. These communications have also

evolved over time and are now including instances of ongoing interventions at the expense of covertness to raise awareness about the current dangers on these marketplaces (Cyjax, 2020c). It is important to note that certain private organisations have very large followings (POI-W5) and that this could be used to their advantage when raising awareness and encouraging further action, as individual followers might become more concerned about these issues and actively denounce them. This idea of social control stems from Becker's study of drug users in the 1960s and some people's opposition to such consumption due to moral principles, leading him to name them 'moral crusaders' (Becker, 1963). In this case however, the trade of illegal drugs and wildlife is not a 'repugnant transaction' (Roth, 2007) only affecting the people involved which others morally disagree with, but rather a transaction that has deep and long-lived impacts on national economies, public health, security, and ecosystems. Upon discovering these issues, such crusaders might start helping these organisations work against 'outsiders' breaking agreed rules, by promoting these ideas in their own networks, raising further awareness, or participating in the policing themselves by reporting illegitimate users and listings or undermining these marketplaces' trust mechanisms, as discussed in the next chapter. In the field of conservation, the perception of others, if they disagreed with the illegal trade of wildlife, was seen to be the most influential tool in reducing demand (Greenfield and Veríssimo, 2018), and the fear of identity and financial theft proved to be an effective message to reduce demand for drug products (POI-D6). Indeed, demand reduction was named by most interviewees and many experts in the literature as the best way to thwart criminal trade (Challender et al., 2014; Greenfield and Veríssimo, 2018; Wallen and Daut, 2018; Veríssimo and Wan, 2019), because as long as there is demand, vendors will find a way to make money from it (POI-D6). These online influencers, as social media is often the most effective way to share educational messages widely, therefore need to be reached and recruited through causes and publications like these. Raising awareness through posts and reports should also aim to spark further action from organisations and individuals lending a hand in these efforts.

The answer to our second research question is therefore that private organisations and individuals perform four main tasks when policing online illegal drug and wildlife trades. First, they scour the Internet and gather information about potentially illegal listings or criminal users. Then they share their intelligence with the Police, legal platforms, and other private

organisations so the relevant groups have all the pieces of the puzzle and can take further action. Private organisations and individuals also provide expertise to the Police and legal platforms to assist them in their interventions with specialised knowledge and skills only they possess, training them and building their capability on these matters. Finally, private organisations inform their clients and the general public about these trades through regular news articles, reports, and blog posts

The answer to our third research question is that private organisations' and individuals' activities are the same when policing both online illegal drug and wildlife trades. However, private organisations are overall less involved in raising awareness about online illegal drug trade, as many publications are already available from the Police and Customs. All of these private organisations' and individuals' activities are summarised alongside the activities conducted by the Police, legal online platforms, and cybercriminal traders in the policing script devised in the Discussion chapter.

Despite this difference in awareness raising activity, the ways these policing activities can be rendered more effective are similar for both products.

6.3 The future of private organisations and individuals

Similarly to the Police and legal online platforms analysed in previous chapters, collaboration and multi-disciplinarity were common themes among private organisation interviewees and documents. However, these collaborations have not occurred without their challenges.

Many interviewees expressed a need for multi-disciplinarity as part of their work. Indeed, the Internet being a vast engine with no boundaries, no single entity or sector can work on this policing alone (POI-D4) and everyone needs to come together to reach this common goal of security (POI-D1).

> *"I think everyone has their role to play, and part of that obligation is understanding what your role is, what it is that you can do, and how you can best assist everyone else in solving the issue of cyber insecurity. You know, it's the same thing with roads, road safety is an issue and everyone has their place to play, it's not just an issue for traffic Police officers to stop and arrest people who are speeding, it's everyone who gets behind the wheel of a car. You need to respect rules of the road and not speed, not run people over, not bump into other cars. And similarly, if you're a pedestrian and you want to cross the road, you can't just run out into the road, you have to know how you can help keep yourself safe, how you can keep other road users safe." (POI-D1)*

Various groups will ideally involve different points of view, individuals with different skills and expertise, toolsets and ideas that would help solve this problem (POI-D1). Cybercrime in general, and Darknet markets in particular, cannot be disrupted entirely by the Police, private industry, non-profits, or academia; all entities need to work together to have a fighting chance (POI-D2; POI-D4).

> *"I can't think of any cybercrime that has been solved entirely by law enforcement, I don't know if that's possible to be honest, without any external data or help. And likewise, no cybercrime could be solved entirely by industry. It has to be both of them working together." (POI-D2)*

"I don't think anything we have provided has been the sole bit of evidence that has solved an investigation, it's certainly a case of piecing bits together, combining what we've got with what law enforcement themselves have got." (POI-D4)

In this context, it was important for some interviewees to understand others' viewpoints in order to collaborate more effectively and ensure they got what they needed out of the relationship. As such, a non-profit organisation tried to understand the needs of the government before designing a training project (POI-W2), and a researcher tried to understand how Police officers work, the constraints they have, and the support they need, to only share with them the most relevant insights (POI-W1). A non-profit organisation also aimed to create opportunities for meetings and information exchange between the Police and legal platform administrators so they would understand the challenge the other is facing and how they could best help one another (POI-W5).

In these kinds of collaborative environments, especially with such sensitive information and sectors participants might not be familiar with, trust is paramount. Private companies working alongside the Police have been building trust after years of working together and developing "*phone call friendships*" (POI-W2) and using each other's first names (POI-D2). They admit they now wouldn't reach out to agencies they have never worked with before or know nothing about (POI-D2). The same can be said for academics being welcomed by the Police in certain meetings that would usually be closed to externals, as they are able to add value and provide another perspective and expertise (POI-W1). Private organisations working together also need to trust each other to ensure information will not be leaked for one player's advantage. Indeed, one interviewee reported that some for-profit organisations try to get an edge and monetise sensitive information for their own gain, by writing about it in their blog for instance (POI-D3). Advertising their involvement in a specific operation, however, could jeopardise its progress. Interviewees therefore admitted to only working with trusted individuals, no matter the companies they worked for (POI-D3), meaning time and personal relationships are more relevant to trust than reputation in this case.

"It can be quite difficult for us when we are working to support others and the information might be quite sensitive […] and we don't necessarily want to give a for-profit the edge in a commercial sense. We don't want them to monetise any

> *sensitive information that we might have and we don't want them to blog about the operation. So that can be quite tricky when you work with a for-profit because they obviously have an incentive to blog and say 'we were a part of this', and sometimes they jump the gun and can compromise an operation. So we are quite careful and we will only work with trusted individuals." (POI-D3)*

Some interviewees mentioned that although private organisations are "*not so competitive they are unable to talk*", they "*are all private companies looking to expand*" (POI-D4) and that they need to strike a balance between collaborating with competitors and still having a commercial product (POI-D5), limiting the extent to which they work with and trust one another. Upon starting an educational group related to drug use, its abuse, and addiction recovery, involving organisations from various industries "*it was painful, because no one wanted to talk*" (POI-D6), everyone was holding on to their secrets. But relationships and trust were built over time and, nearly a decade on, conversations are now much more forthcoming (POI-D6). Indeed, for issues such as drugs and wildlife, which have impacts on health, economies, and security, while independent action is a good starting point, "*what better way [is there] to reach consumers than to say we work with competitors and all do it together*" (POI-D6).

Beyond the issue of competition between similar organisations, collaboration between different organisations has also proved challenging, as many interviewees and their organisations do not trust other entities' skills and motives in this policing arena and they do not understand their ways of working. As such, a researcher reported legal platform administrators had no interest in any academic input (POI-W1), and the Police were less likely to trust and work alongside non-profits as they relied on emotions more than facts (POI-W1) [these claims were not corroborated by Police officers who mentioned how helpful some non-profits had been in their work (P-W4)].

> *I generally work with law enforcement, I don't work with industry as such. I tried engaging with eBay and they're just not interested, just like Facebook aren't interested. (POI-W1)*

Legal platform administrators were also accused of lying about the number of listing takedowns they report (POI-W1) and academics were described as "*not geared up to support the Police generally speaking*" (POI-W3). In the realm of drugs, it was noted that when the opioid crisis hit the US, companies in various industries were all too quick to blame others (POI-D6). For instance, pharmaceutical companies pointed the finger at technology companies which made it possible to procure these drugs online and vice versa (POI-D6).

This failure to cooperate for mutual benefit shouldn't however be seen as a sign of ignorance or irrationality, as much of game theory is based on this very phenomenon (Putnam et al., 1993). All parties likely have their reasons for not collaborating with others in this case and many, being aware of this shortcoming, will work towards that goal of further collaboration in the future (POI-D4). The ones that already do collaborate are likely to continue to do so building on their positive results, which might also influence other organisations to follow suit. Indeed, following the recent arrest of a high-level wildlife trafficker in Thailand after a five-year investigation, the WJC commented that "this case demonstrates the results that can be achieved when public-private partnerships work together to detect and disrupt transnational organised wildlife crime" (WJC, 2021).

Although systems and communication channels have been put in place for private organisations to collaborate, and some do, different actors have conflicting aims which are currently preventing them from fully collaborating. The answer to our fourth research question is therefore that increased collaborations between private organisations and other policing actors in the public and private realms, for information gathering, intelligence sharing, expertise provision, and awareness raising can further increase the effectiveness of online illegal drug and wildlife trades policing. These collaborations are at the centre of the policing script presented in the Discussion chapter, as it is argued understanding the goals and skills or other entities will spur further collaborative interventions in the future.

6.4 Conclusion

This chapter presented an exploratory study into the role of private organisations and individuals in different sectors and their contribution to the overall policing of the online illegal trades of drugs and wildlife through the use of expert interviews and the content analysis of private organisations' publications.

Private organisations and individuals participate in the policing of the online illegal trades of drugs and wildlife by gathering information about illegal trades and traders on various part of the Internet, sharing relevant intelligence with the Police and legal platforms, providing them with their expertise to support their interventions, and raising awareness about these trades.

This chapter was divided in three parts: the first part presented findings about the private organisations and individuals involved in the policing of these trades; the second part then analysed the activities these private organisations and individuals perform and how these differ between the policing of online illegal drug and wildlife trades; and the third part discussed how private organisations and individuals can be more effective in this type of policing in the future.

Although they act more behind the scenes than the Police or even legal platform administrators do, private organisations and individuals are one of the pillars of online illegal drug and wildlife trades policing, given the many activities they perform and the connections they are able to draw with other groups. Despite needing to remain more covert in their involvement, this chapter provides some understanding about their continued importance in this policing arena. Contrary to drug policing where the Police is more dominant, the policing of online illegal wildlife trade appears to be more private-led, likely as a reaction to the lack of Police attention and the importance the wider public places on this issue (Button, 2019). However, private organisations and individuals also hold a place in the policing of online illegal drug trade, as these organisations and individuals complement the actions of the Police due to their additional resources and expertise, as shown in this thesis' policing script.

Alongside private organisations and individuals, this thesis argues cybercriminal traders have supported the Police indirectly on Darknet markets. They are the subject of the next chapter.

7 Cybercriminal traders

Darknet markets have been defined as enabling the sale of illegal goods and services online (Décary-Hétu and Giommoni, 2016). These online marketplaces are now increasingly privileged over offline ones for illegal trade, due to the large range of products, reduced prices, and protection from violence and threats they offer to buyers, and the anonymity and financial opportunities they provide to vendors and administrators (Van Buskirk et al., 2014; Barratt et al., 2016; Décary-Hétu and Giommoni, 2016; United States Court of Appeals for the Second Circuit, 2016). The Police have therefore been charged with disrupting these Darknet markets in order to reduce illegal trade and have made this threat a priority (Europol, 2019g).

Two of the methods employed by the Police have been to take down Darknet markets' infrastructure and arrest their administrators, as was the highly publicised case for Ross Ulbricht and the Silk Road in 2013 (Van Buskirk et al., 2014; Bilton, 2018). Responses to these interventions have been analysed and these techniques have been criticised for leading to the displacement of cybercriminal trade at later times, on other marketplaces, or through other traders (Yip, Webber, et al., 2013; Van Buskirk et al., 2014; Décary-Hétu and Giommoni, 2016; Hutchings et al., 2016; Paquet-Clouston et al., 2017; Van Buskirk et al., 2017; Ladegaard, 2018). However, rising distrust between traders has also been observed following recent Police arrest and takedown successes, as well as the voluntary exits administrators performed to avoid their marketplaces being shut down (Europol, 2021e).

Other policing methods discussed more recently with regards to Darknet market policing include slander and Sybil operations, aimed at instilling mistrust between traders by respectively leaving false feedback to vendors and making fictitious reputable accounts default on their trades (Décary-Hétu and Dupont, 2013; Yip et al., 2013b; Hutchings and Holt, 2017; Paquet-Clouston et al., 2018). These operations replicate scamming and exit scamming behaviours exhibited by cybercriminal traders themselves on these marketplaces, which are discussed in the documents analysed in the Police and Private organisations and individuals chapters. These operations aim to leverage weaknesses in the marketplaces' reputational mechanisms in order to decrease cooperation and trust among traders, as has been shown is a result of scamming and exit scamming following which users take some time to trust marketplaces again (Soska and Christin, 2015). However, unlike takedown and arrest

operations, these tactics have only been discussed at a conceptual level and little empirical research has been undertaken about their effectiveness, due to the number of practical and ethical challenges of performing such research on real marketplaces.

The aim of this study is therefore to understand whether and how cybercriminal traders contribute to Darknet market trade policing to better situate this group in the cyber policing classification and policing script devised in the Discussion chapter.

This chapter presents the pilot results of a social laboratory experiment performed in November 2019 at the University of Oxford Centre for Experimental Social Sciences (CESS) at Nuffield College. The experimental design replicated an online illegal marketplace, a "market for lemons" where buyers don't possess any information about the quality of products and services for sale or about the intentions of vendors, in order to observe participants' behaviours and decision-making when these interventions were made, as well as gauging these operations' effectiveness in decreasing trust among participants based on these results. Although illegal trade also happens on legal platforms, such tactics are not used there so as not to discourage legitimate trade, so Darknet markets are the sole focus of this chapter.

As the actors under scrutiny in this chapter are not willing contributors to the policing of online illegal drug and wildlife trades and their activities have already been detailed (e.g. scams, exit scams…), the research questions investigated as part of this thesis are slightly reformulated to fit this chapter's policing category. Indeed, this chapter aims to ascertain whether cybercriminal traders play a role in the policing of their own marketplaces and if so what the consequences of their actions are. This chapter therefore aims to answer the questions:

1. What disruptive consequences do cybercriminal traders' activities have on the Darknet market ecosystem?

   1.a. Do slander and Sybil operations have an impact on the prices offered by cybercriminal vendors?

   1.b. Do slander and Sybil operations have an impact on the prices chosen by cybercriminal buyers?

1.c. Do slander and Sybil operations have an impact on the quality produced by cybercriminal vendors?

1.d. Do slander and Sybil operations have an impact on cybercriminal traders' buying and sending decisions?

1.e. Do slander and Sybil operations lead to a decrease in trust between cybercriminal traders?

2. Are cybercriminal traders involved in the policing of online illegal drug and wildlife trades?

In order to answer the aforementioned questions, this chapter is divided in three parts, each one focussing on different research questions. The first part describes previous market experiments and the specific focus of this experiment on slander and Sybil operations as a way to answer this thesis research questions; the second part then details the consequences of the slander and Sybil interventions on the prices offered, purchase prices, quality offered, buying and sending decisions, and trust between experiment participants; and finally the third part argues that cybercriminal traders should be considered policing participants in the online illegal trade policing context.

7.1 Social laboratory experiments in cybercriminal context

The researcher conducted a social laboratory experiment to test participants' behaviours and decision-making following slander and Sybil interventions, a method which is newly applied to the field of cybercrime research.

7.1.1 Market experiments

The main component of this experiment was a market game, however before detailing the specifics of this design, it is important to note the market experiment tradition that precedes it. In *The early history of experimental economics*, Roth (1993) explores the first three strands of experimental economics. Following theories of individual choice and game theory with the first version of the Prisoner's Dilemma, the third strand was the organisation of markets at the core of supply and demand theory with the works of Chamberlin (1948) and Siegel and Fouraker (1960). The former posited that market outcomes could differ from a theoretical competitive equilibrium, a theory which he tested experimentally, and results confirmed that the number of units transacted by participants was greater than the competitive volume and their average price below competitive price (Chamberlin, 1948). The latter experimentalists designed bargaining games where pairs of participants had to reach an agreement over a product price and quantity given various amounts of information about their own and the other's payoffs, showing an increase in information led to increased choices of optimal price and quantity for both participants (Siegel and Fouraker, 1960). Since then, market experiments have gained acceptance and recognition in the field of economics and have evolved in many different directions following theory and policy developments (Noussair and Tucker, 2014).

Of particular interest to this study, one of these directions has been the building of trust in online markets since the early 2000s, following the emergence of platforms such as eBay, and testing the effectiveness of reputational mechanisms and their benefits, a research area sparked by the high levels of fraud observed compared to offline trade (Ba, 2001; Dellarocas, 2001; Ba et al., 2003; Bolton et al., 2004). The common thread among these studies was to find or confirm ways to increase trust on these platforms. As such, Bhattacharjee and Goel (2005)'s study focussed on bad mouthing and ballot stuffing – the legal market equivalents of

slander and Sybil operations – findings ways to avoid these practices and ensure reputational systems remained resistant to these attacks and meaningful to their users. Avoidance is an understandable strategy when it comes to legitimate markets, as users were encouraged to join despite their novelty. However, this is not the case for online illegal markets. Building on Franklin et al. (2007)'s slander and Sybil concepts, Hoe et al. (2012) started to investigate the lemonisation of cybercriminal markets - "the drive of real crime products and services out of the market by lemons" (p.61). Their study did not involve participant experiments, but game theoretical frameworks such as cost functions which simulated lemonisation. They concluded that lemonisation could happen on such markets if slander and Sybil operations were conducted on peaches, high-quality products researchers were trying to drive out by adding noisiness to quality signals, rather than focussing on lemons, which were already inexistent or low-quality products (Hoe et al., 2012). This study was then followed by theoretical insights by Yip et al. (2013b) and Decary-Hetu and Laferriere (2015) arguing for enforcement operations centred around slander and Sybil interventions due to their potential longer-term impact than cybercriminal arrests and market takedowns. Following their theoretical study of GhostMarket data, Decary-Hetu and Laferriere (2015) advocated for Criminology academics to work with Computer Science ones in order to create computer simulations of behaviour models and provide better estimates of traders' responses to such operations. This project conducted an experiment with human participants to that effect.

7.1.2 A focus on slander and Sybil interventions

Social laboratory experiments were applied in the case of this thesis in order to test Darknet market users' responses to slander and Sybil operations conducted by the Police on these marketplaces, but not scientifically testable in the natural world. While there are several ways to apply social laboratory experiments in this case, this chapter focusses on the impact cybercriminal traders have on their own marketplaces through their financially-motivated and self-serving behaviours. This study also increases our understanding about whether negative consequences from these behaviours could be replicated at scale when deployed by the Police, in this case researching the destruction rather than the building of trust. This experiment therefore focusses on slander and Sybil operations instead of researching interventions such as arresting cybercriminal traders or taking down markets to observe

relocation, which would be more appropriate in a Police-centred experiment. Participants in industry speak highly of slander and Sybil operations, as they mention trust is more difficult to rebuild than infrastructure (POI-D2). Exit scams performed by market vendors and administrators have helped this strategy, as "*people themselves have become less trusting and that just erodes communication*" (POI-D2), which markets such as these rely on for success (P-D2). The need to test these operations further is therefore paramount in this endeavour, as well as trying to ascertain whether cybercriminal traders might in fact be the most effective actors in disrupting cybercriminal trade.

As this is the first social laboratory experiment conducted to replicate interventions on Darknet markets, the design detailed below remains basic, not including various volumes of trade, buyer motivations, or different levels of 'compromises'. These features could be added to future experiments to test their specific impact, as well combining them with Police interventions to observe any combined effects, such as preventing some participants from continuing to trade in the way of arrests, or providing several fictitious marketplaces for participants to relocate to if some were seen as more or less risky.

A table summary of the games contained in each experiment is presented below:

Table 7.1: Summary of experimental games

	Trust game 1	Market real ratings	Market compromised ratings (slander)	Market real defaults	Market compromised defaults (Sybil)	Trust game 2	Survey
Control	X	X		X		X	X
Slander	X		X	X		X	X
Sybil	X	X			X	X	X

Each session involved playing an initial trust game, a variation of a "market for lemons" game, a second trust game, and then filling in an end-of-experiment survey. Each of these games is described below and positioned within a larger experimental and cybercriminal trade context.

Participant instructions (Appendix D.1) were provided in paper and digital form to all participants and read aloud by the researcher at the start of each session to ensure all participants were aware of them and knew the others were too. With the exception of the final survey, each of the following games was tried by participants once before the 'real' games began, as is considered good practice in the field (Friedman and Sunder, 1994). Participants were always informed when they were playing 'trial' or 'real' rounds. Each experiment consisted of trust and "market for lemons" games.

For the trust games, each participant was first randomly paired up with another participant in the session. Participants remained anonymous to prevent reputational effects at this stage (Kreps et al., 2003), though players knew their counterpart was real rather than computerised, as this was likely to have a positive effect on trust (Johnson and Mislin, 2011). Both participants received tokens in order to cancel the feeling of inequality (Adams, 1965) - the first mover decided what share of their tokens to send to their counterpart, the counterpart then received triple that amount and decided how much to send back to the first mover (see First task in Appendix D.1). Participants were then randomly re-matched and played the other role, so they experienced both sides of the game without the possibility of punishing their partner for the previous game. This sequential game was similar to buyers paying for purchases without guarantee that the product will actually be sent and be of good quality, such as in markets like eBay (Resnick and Zeckhauser, 2002), putting their blind trust in the other with no promise of return (Berg et al., 1995) - "…he that performeth first, has no assurance the other will perform after" (Hobbes, 1651). This game was therefore used at the start of the experimental session in order to measure trust between participants before the main game began and was used again after it in order to evaluate how such trust evolved during the "market for lemons" game. The results of all trust games were given at the end of the session so as not to influence participants' behaviours during the remainder of the experiment.

Online illegal markets, and Darknet markets specifically, have been likened to "markets for lemons" due to their characteristics of information asymmetry (Hoe et al., 2012), no credible quality disclosure, the presence of rippers, market participants who do not provide the goods and services that have been paid for, and lack of quality assurance and regulation (Herley and

Florencio, 2009). Participants therefore took part in "market for lemons" trading games based on Holt and Sherman (1999)'s classroom game and the basis of Chen's (2019) pre-programmed game on the oTree software. In this case, the product to be traded remained unnamed and neutral, in an effort not to burden participants with a criminal product. This was not seen as an issue as the underlying economic principles remained and the results were then transposed to cybercriminal trade. Participants were assigned a fixed role throughout this task, vendor or buyer, and were randomly grouped with two other members in the session. In each trio, one participant was the buyer and the other two were vendors. It is noted that in economic terms, this setup resembles that of an oligopoly, a state of limited competition, in this case a duopoly. This has been criticised in the experimental literature for leading to collusion between the two vendors and therefore impacting prices, which would be more difficult to achieve in markets with more vendors (Huck et al., 2004). However, three-participant groups in this experiment were re-matched after each round and for the total of 30 rounds, limiting the opportunities for collusion between vendors, who also did not have access to the price offered by the other vendor in their group. At the beginning of each trading round, all the participants received 50 tokens. Vendors began by privately choosing a price and a quality grade for their products. The grade could be High, Medium, or Low; higher grades cost more to produce and were worth more to buyers. Buyers then had a chance to purchase from one of the vendors at the price listed or not to buy anything. Before purchase, buyers could not observe quality grades and vendors could not signal any quality. After purchase, the price and grade of the bought unit were revealed to them, as well as the vendor's decision to 'send' the product or not. Not sending products meant vendors enjoyed both their initial endowment and the price of the product without the cost of production (based on Bolton et al. (2004)'s ship or not ship decision following the same payoffs). Buyers would then provide a rating to vendors, which would be visible to future potential buyers and updated after each round. While the parallels with an online marketplace were obvious, no reference was made to the experiment replicating Darknet market conditions specifically, so as not to influence participants' behaviours but instead observing general market dynamics when subjected to these interventions. Payoffs for vendors and buyers were calculated as follows, participants only had access to their own role's payoff calculations (see Appendix D.2).

Table 7.2: Product grades, costs to vendors, and values to buyers

Grade	High	Medium	Low
Production cost	30	20	10
Value to buyer	45	30	15

Buyer payoffs = 50 tokens + value of the grade purchased (if sent) – vendor's price Vendor payoffs = 50 tokens + vendor's price - cost of the grade produced (if sent) Buyers who chose not to buy from either vendor in their group and vendors who were not chosen by buyers in any given round, finished that round with 0 tokens.

Several iterations of these trading games were played by participants in different sessions:

- CONTROL: involved no interventions – vendors advertised their products, buyers chose which vendor to buy from, if any, based on price alone, selected vendors decided whether to 'send' their product or to default, and buyers rated the purchases they had just made after the quality grade of the product was revealed (see Figure 7.1).
- SLANDER TREATMENT: simulated a slander operation by introducing a 15% chance that each buyer's rating was randomly 'compromised' and replaced with another randomly selected rating during each round (see Figure 7.2). Participants were informed of this rate of compromise at the start of the experiment but were not informed if they were affected by it, either as a buyer or as a vendor (see Second task in Appendix D.1).
- SYBIL TREATMENT: simulated a Sybil operation by introducing a 15% chance that a vendor's positive 'sending' decisions was randomly 'compromised', not sent, during each round (see Figure 7.3). Participants were informed of this rate of compromise at the start of the experiment but were not informed if they were affected by it, either as a buyer or as a vendor (see Second task in Appendix D.1).

The Control sessions did not include any interventions in order to compare the achieved results with previous "market for lemons" experiments and ensure the novel addition of the rating and default components to this game yielded similar results and the experiment was

therefore valid. Indeed, “market for lemons” results belong to two similar-sized groups: those showing an increase in prices and decrease in quality, as observed by Akerlof (1970), and those showing decreases in both prices and quality, as observed by Holt and Sherman (1999).

The above ‘compromises’ were inspired by previous experiments’ inclusion of noise in repeated Prisoner’s Dilemma games whereby participants’ choices to Cooperate or Defect were not always implemented (Fudenberg et al., 2012; Arechar et al., 2017; Gallo et al., 2019). Such noise has not so far been included in market experiments, making this addition novel as well as being representative of Darknet market conditions. The 15% compromise level, although it can appear quite high given the amount of trade on these marketplaces and the resources needed in order to achieve such a level in the natural world, was chosen following Espinosa (2019)’s estimate that between 83% and 88% of vendors actually ‘send’ their orders on marketplaces such as Hansa. Instead of being a realistic estimate of the level of slander and Sybil operations the Police might be able to perform on a real marketplace, this compromise level was therefore chosen to replicate the Darknet market conditions created by cybercriminal traders themselves to evaluate participants’ responses.

Of the reviewed market experiments, the inclusion of several rounds in experimental designs was commonplace. Although this experiment involved 30 consecutive rounds, and behaviours from one round likely affected those in another, the constant change in pairings provided neutral opportunities for learning. Indeed, when testing the efficacy of feedback mechanisms on three groups – a strangers market where participants were re-matched to new players during each round, a feedback market where participants were re-matched to new players but had access to a historic of the vendors’ decisions to ship or not to ship their product, and a partners’ market where pairs remained fixed and were given a historic of decisions - Bolton et al. (2004) concluded that the partners’ market performed better than the feedback market, as trust was built between partners. This experimental design therefore prevented trust from being built between specific pairs, which would have increased learning further. Additionally, while testing players’ ability to learn to cooperate in repeated Prisoners’ Dilemma games, Bereby-Meyer and Roth (2006) found that the noisiness (tampering) of payoffs substantially reduced cooperation among fixed pairs but that the rate of cooperation decay was slower for participants who were re-matched with a succession of one-time opponents. This experiment

therefore allowed for a lengthier decision-making process with regards to trusting and cooperating with one's partners. Between both of the above conditions, the experiment ideally reached a neutral learning level.

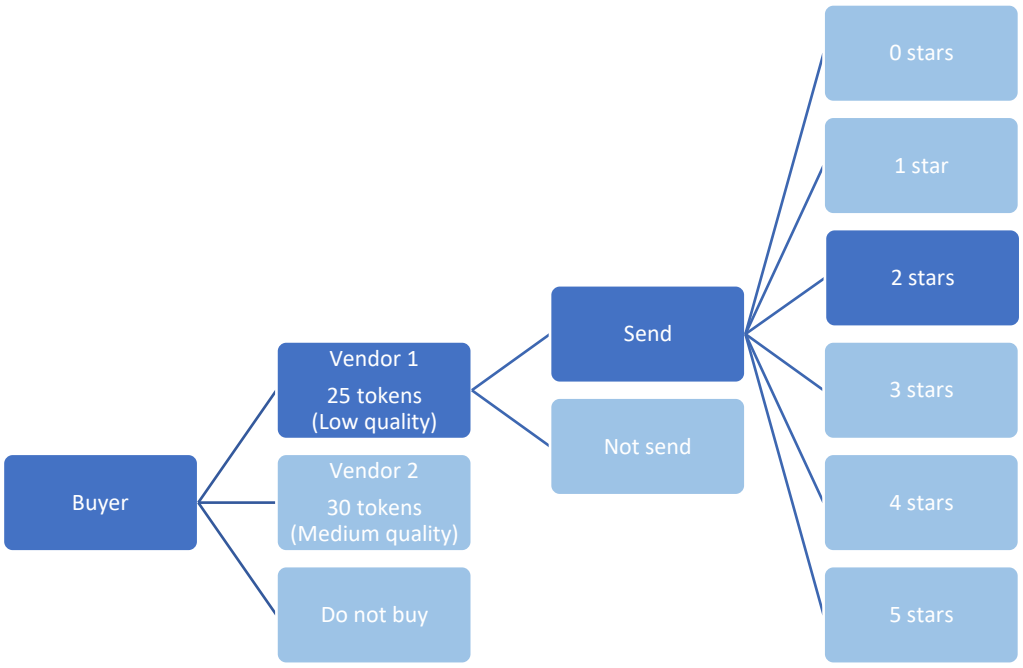


Figure 7.1: Control decision sequence

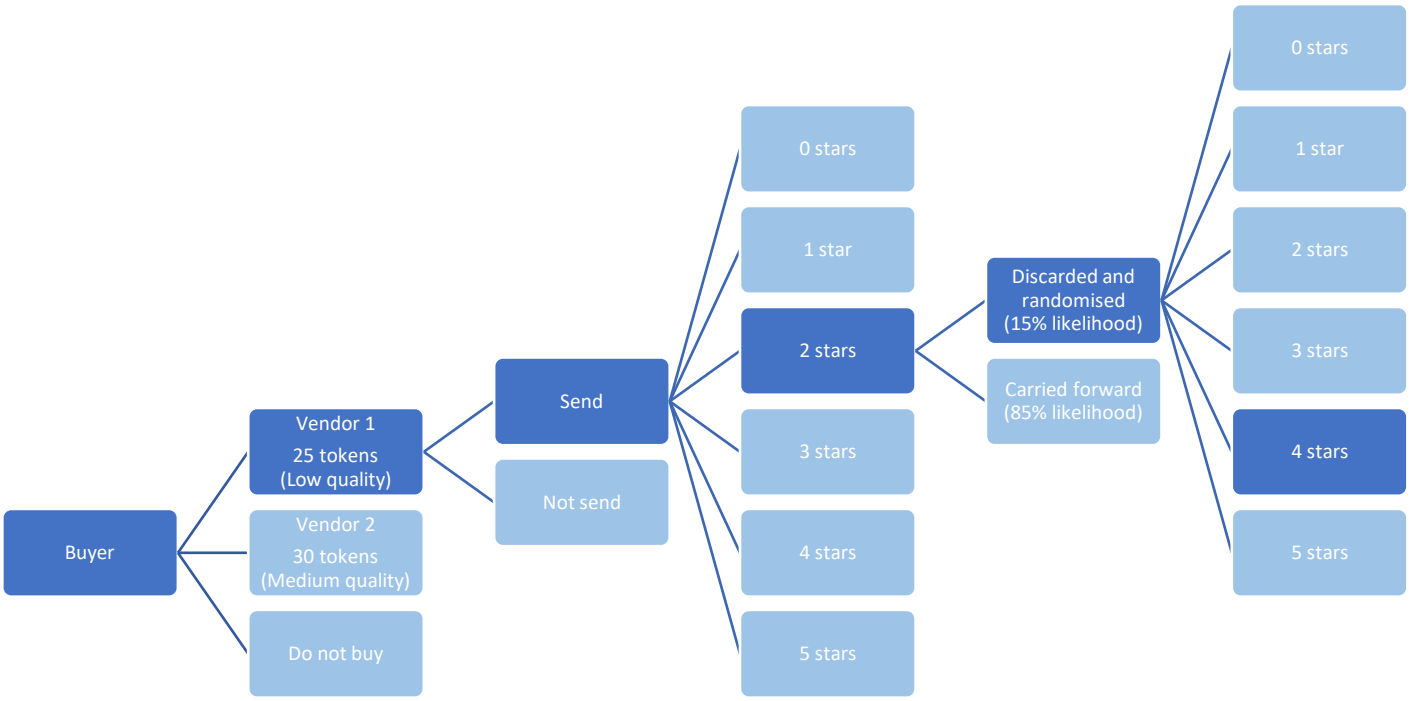


Figure 7.2: Slander treatment decision sequence

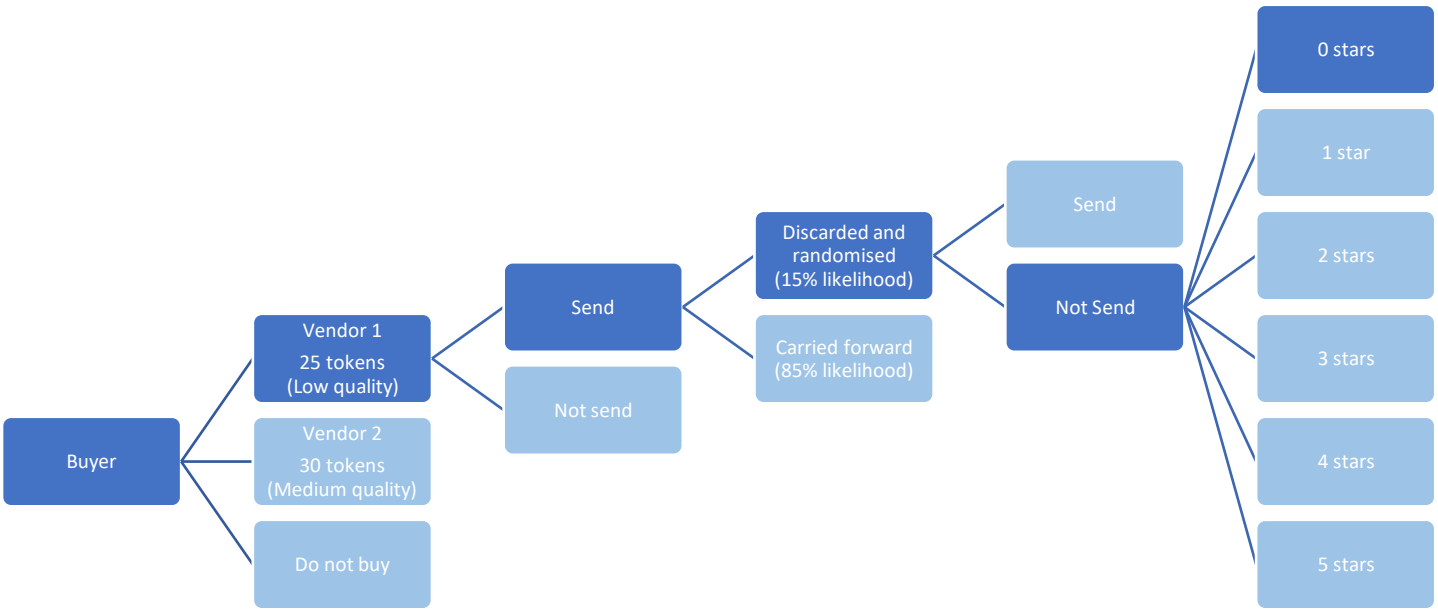


Figure 7.3: Sybil treatment decision sequence

Finally, participants were asked to complete a survey while their monetary rewards were prepared at the end of the session. These surveys not only sought demographic information about participants, but also their perceptions about the experiment. Indeed, Webster and Sell (2007) believe that questionnaires should always be included in social laboratory experiments in order to better understand the participants' comprehension of and engagement with the experiment, what they were asked to do, and how they and other participants did it.

Recent experimental research shows that a lack of reputational information decreases cooperation in markets that rely on bilateral exchange (Gallo and Yan, 2015). As a result, the researcher hypothesises that, when slander and Sybil interventions are carried out:

H1) Prices offered by cybercriminal vendors will decrease;

H2) Purchase prices chosen by cybercriminal buyers will decrease;

H3) Product quality offered by cybercriminal vendors will decrease;

H4) Cybercriminal traders' decisions to buy and send products will decrease;

H5) Trust between cybercriminal traders will decrease.

The overall expectation is therefore that cybercriminal traders have been and could continue to be instrumental in the policing of their own marketplaces, as adverse responses are elicited following these interventions. To this effect, this chapter suggests the addition of another category to supplement Button (2019)'s classification which would take into account any individuals or groups who unwillingly participate in policing by their actions and the knowledge and tools they indirectly provide to the Police and Private Police to help their interventions. This category is discussed further and mapped in relation to already-existing categories in this thesis' Discussion chapter.

7.2 Disruptive consequences of cybercriminal behaviours

This section presents the findings gathered from the above experimental design, including behavioural consequences related to the prices offered, purchase prices, quality produced, and buying and sending decisions during the "market for lemons" game, as well as during the trust games. Medians are reported in the case of non-normally distributed data, as they better represent what non-parametric tests are testing. Indeed, means are otherwise biased by outliers in the datasets.

7.2.1 Prices offered

The median price offered by vendors in the Control sessions was 22.5 tokens, compared to 15 tokens in slander sessions and 20 tokens in Sybil sessions, representing a price drop of 7.5 tokens in relation to the slander operation and of 2.5 tokens for the Sybil operation. Boxplots are used alongside non-parametric tests in order to visually observe such differences between groups (see Figure 7.4).

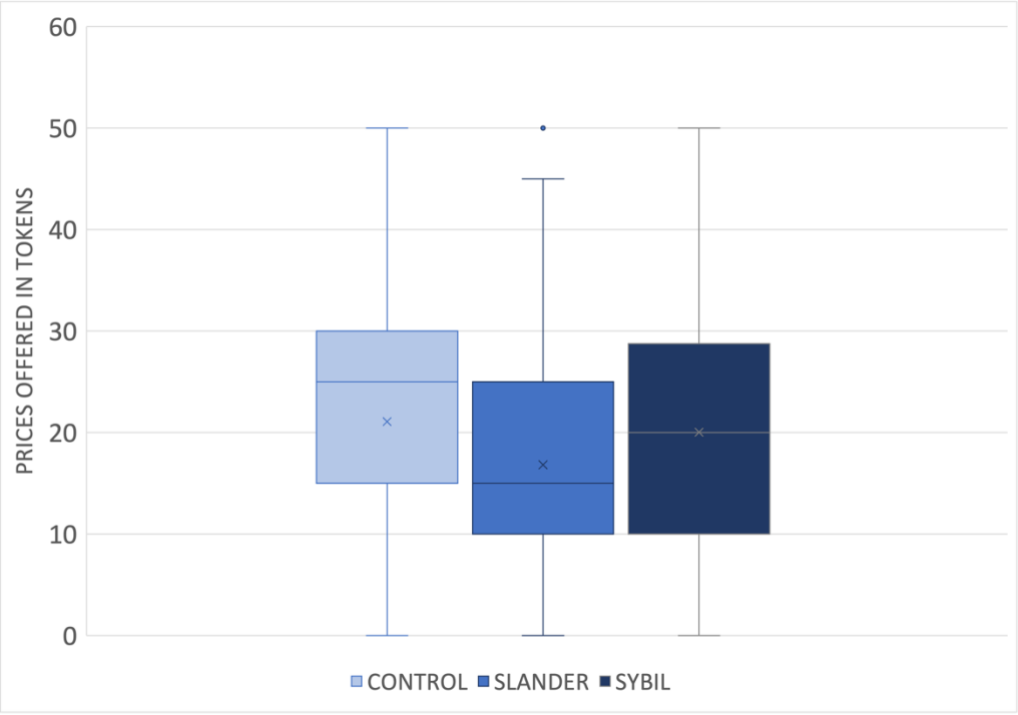


Figure 7.4: Boxplot for the prices offered by vendors during the "market for lemons" game in Control, slander, and Sybil sessions

Overall, after comparing the 2,760 data points gathered throughout Control and treatment sessions, prices offered were significantly affected by slander and Sybil interventions ($H(2)=77.1$, $p=0$). These results show a H statistic larger than the associated critical Chi-Square value for a sample involving 2 degrees of freedom (number of groups -1), and a very significant difference between the groups, as a p-value of 0 suggests there is no chance both samples could have originated from the same population. Mann-Whitney U tests were conducted to follow-up on these significant Kruskal-Wallis results. It appeared that prices offered in the slander treatment were significantly lower than those offered during the Control ($U = 311,089$, $p = 0$). Indeed, when all 1,800 prices offered throughout rounds in Control and slander sessions were ranked, slander prices corresponded to a mean rank of 960, compared to a mean rank of 1,010.16 for Control prices. Prices offered in the Sybil treatment (mean rank = 867.71) were also significantly lower than those offered during the Control (mean rank = 938.66, $U = 371,149$, $p = 0.003$). Finally, prices offered in the slander treatment (mean rank = 885.29) were significantly lower than those offered during the Sybil treatment (mean rank = 1,035.71, $U = 533,005.5$, $p < 0.001$) when comparing these 1,920 data points. The null hypothesis of no difference is therefore rejected for all three groups.

Additionally, prices were also driven downwards throughout the experiment. Indeed, overall, prices decreased by 41% throughout rounds in the Control sessions and 33% in slander and 40% Sybil sessions, calculated between the median prices in the first round and the very last round. This final round was the lowest pricing point in the Control session. However the lowest median pricing point in slander sessions was 10 tokens in Round 16, which represented a 67% decrease from the original pricing point. Similarly, the lowest median pricing point in Sybil sessions was 12.5 tokens in Round 27, which represented a 50% decrease from the original pricing point (see Figure 7.5).

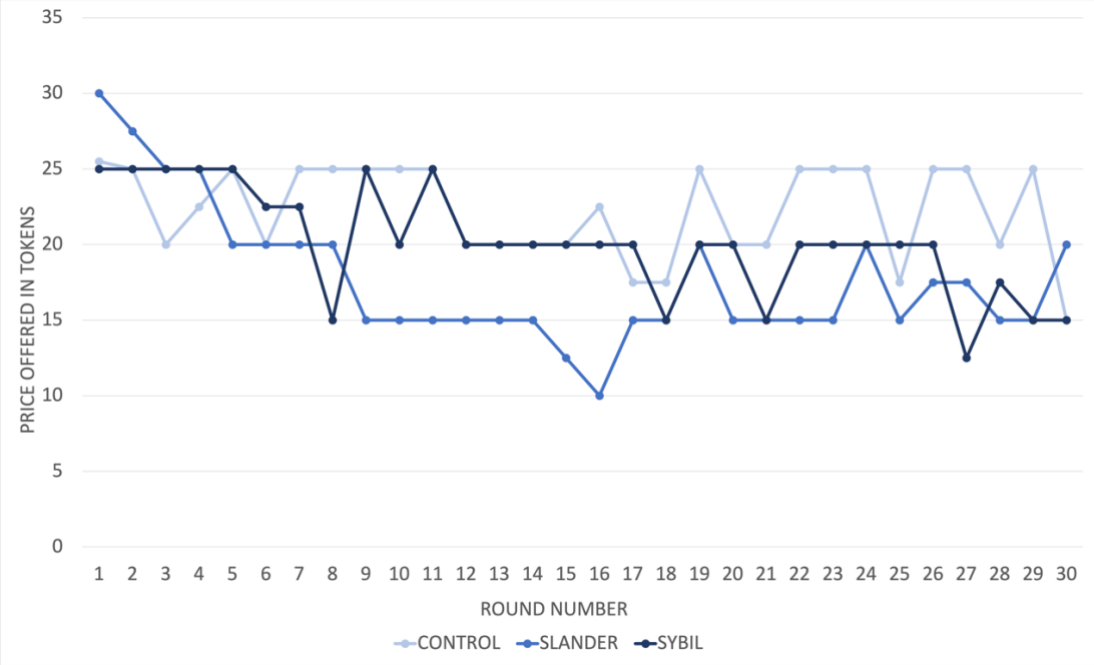


Figure 7.5: "Market for lemons" evolution of median prices offered by vendors throughout rounds and across treatments

Across all treatments, there were two common pricing strategies (see Appendix D.3) – pricing Low (as low as 0 or 5 tokens), likely to encourage buyers to make a purchase despite uncertain qualities, and pricing High (as high as 45 or 50 tokens), potentially to signal quality to buyers in some way. The former strategy could be explained by the need for vendors to make a sale to have a chance of earning payoffs (compared to getting 0 tokens if they were not chosen for the sale), encouraging them to sell products at a small margin in order to create an initial reputation for themselves and help secure future purchases based on their ratings. Indeed, many products were sold for 0 or 5 tokens (out of 50) and produced at Medium or High qualities. Both strategies were ultimately successful depending on the buyers on the other end on these trades. Throughout the experiment, regardless of participants' preferences and behaviours, overall prices offered by vendors for their products also decreased in slander and Sybil treatments, although more sharply in the former than in the latter.

The answer to research question 1.a. is therefore that slander and Sybil operations, in the case of this experiment, both had an impact on the prices offered as shown by significant decreases compared to the Control sessions, although slander interventions decreased prices further. Our first hypothesis that the prices offered by cybercriminal vendors will decrease is therefore confirmed as both slander and Sybil operations decreased prices offered.

7.2.2 Prices purchased

Although the prices at which buyers decided to buy were dependent on the prices offered by vendors, buyers still had a choice between two offers during each round. It is therefore interesting to understand which price points buyers chose for their purchases.

The median purchase price chosen by buyers in the Control sessions was 20 tokens, compared to 15 tokens in slander and Sybil sessions, representing a price drop of 5 tokens in both cases (see Figure 7.6). All of these are therefore below the median prices offered by vendors in each treatment, signalling buyers chose the cheapest offers overall.

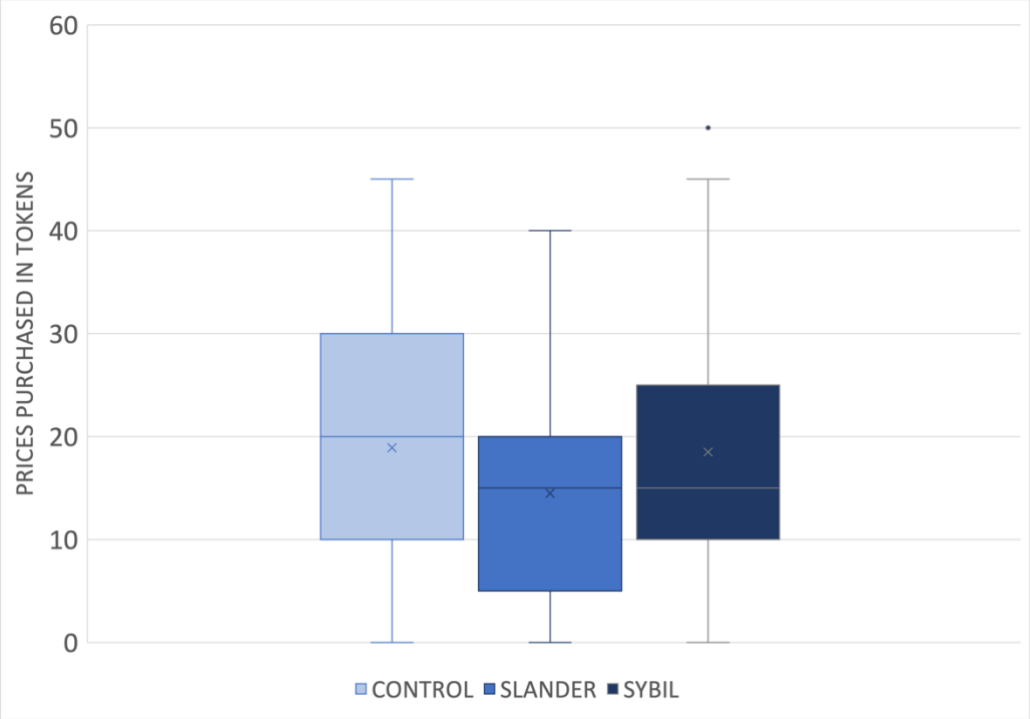


Figure 7.6: Boxplot for the prices purchased by buyers during the "market for lemons" game in Control, slander, and Sybil sessions

Overall, after comparing the 1,368 data points gathered throughout Control and treatment sessions, prices purchased were significantly affected by slander and Sybil interventions ($H(2)=46.7$, $p < 0.001$). The non-rounded sample size reflects the few buyers who chose not to buy any products during various rounds, as explained further in a later section. Sample sizes also varied between sessions, not only because of the smaller number of participants in

the Control sessions compared to treatment sessions, but also because decisions not to buy fluctuated in all sessions. Mann-Whitney U tests were conducted to follow-up on these findings. It appeared that purchase prices in the slander treatment (mean rank = 396.47) were significantly lower than those offered during the Control (mean rank = 501.62, U = 75,273.5, $p < 0.001$). However, purchase prices were not significantly different in the Sybil treatment (mean rank = 437.92) compared to those in the Control (mean rank = 457.46 U = 94,842.5, $p = 0.255$). Finally, purchase prices in the slander treatment (mean rank = 428.01) were significantly lower than those purchased during the Sybil treatment (mean rank = 525.68, U = 136,793.5, $p < 0.001$). The null hypothesis of no difference is therefore rejected for two of the three groups.

The prices at which buyers bought products also decreased throughout rounds and across treatments. Indeed, overall purchase prices decreased by 50% in the Control sessions, 33% in slander sessions, and 60% in Sybil sessions, calculated between the median prices in the first round and the very last round. This final round was the lowest pricing point in the Control and Sybil sessions, however the lowest pricing point in slander sessions was 10 tokens in Rounds 13, 14, 15, 22, 28 and 29, which represented a 67% decrease from the original pricing point (see Figure 7.7).

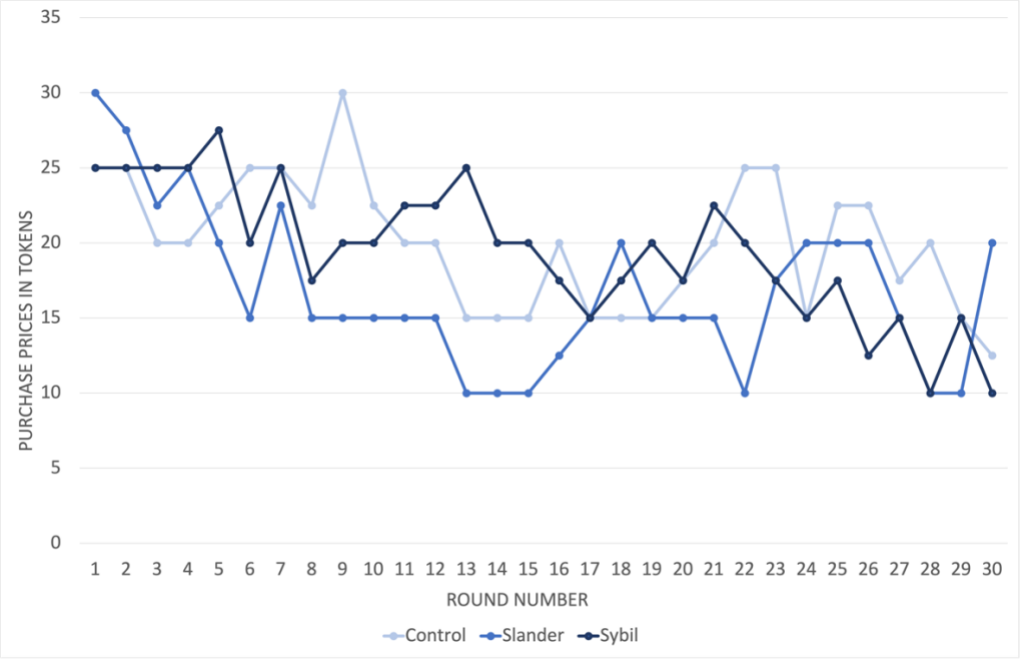


Figure 7.7: "Market for lemons" evolution of median prices purchased by buyers throughout rounds and across treatments

As well as a decrease in the prices offered by some vendors, the experiment also showed a decrease in the prices chosen by buyers for their purchases in slander and Sybil treatments. Indeed, although buyers usually had lower prices to choose from based on vendors' offers, many buying decisions involved buyers choosing between a low price and a high price, as per the pricing strategies detailed previously. In these cases, a few buyers were less risk-averse and chose high-priced products, which could reap bigger rewards, but the majority of buyers chose lower-priced products. Indeed, slander and Sybil participants rated themselves as slightly more risk-taking than their Control counterparts (see Appendix D.5). However, as discussed above, these decisions were not necessarily less profitable as low-priced products were often produced to Medium or High quality standards, going against profit-maximising reasoning for vendors but building up their reputation for the rest of the game. Noticing this, buyers potentially deemed lower-priced products less risky and more profitable and therefore chose them over higher-priced products in sessions impacted by slander or Sybil operations.

The answer to research question 1.b. is therefore that the slander intervention, in the case of this experiment, had an impact on purchase prices as shown by a significant decrease compared to Control sessions. However, the Sybil intervention did not lead to a significant decrease in purchase prices. Our second hypothesis that the purchase prices chosen by cybercriminal buyers will decrease is therefore confirmed as both slander and Sybil operations decreased purchase prices, although only slander operations did so significantly.

7.2.3 Quality offered

As well as decreases in prices offered and purchased, slander and Sybil interventions also had an impact on the quality grades produced by vendors.

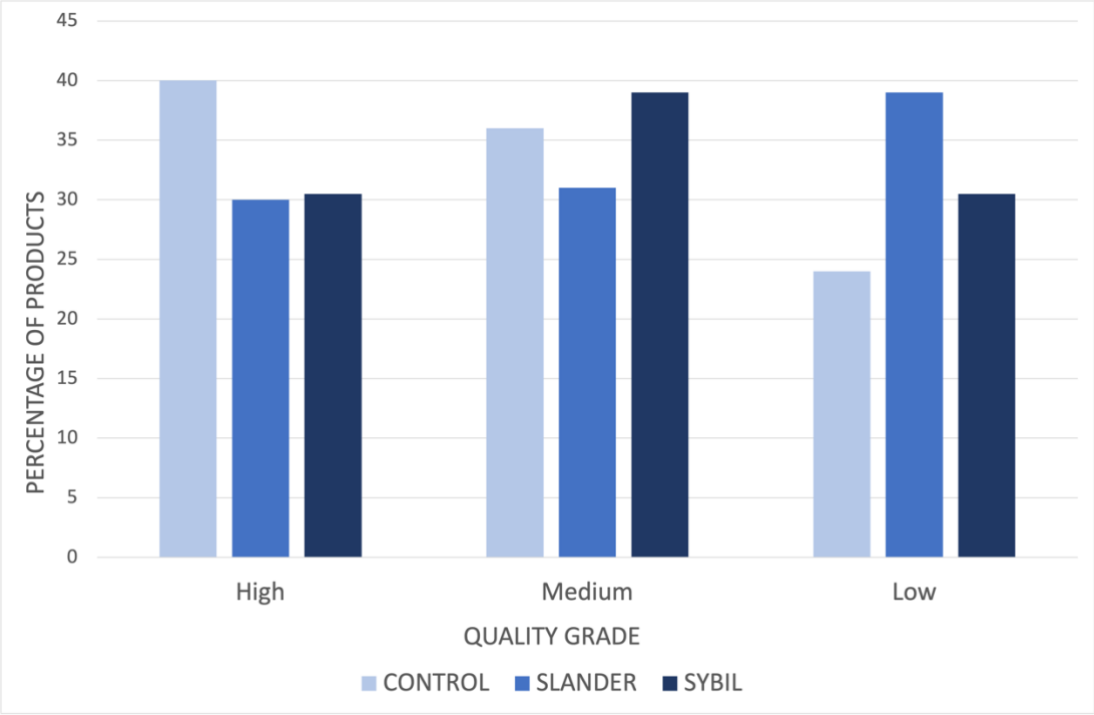


Figure 7.8: "Market for lemons" proportion of quality offered by vendors across treatments

Control sessions were the only sessions in which High quality grades were produced in higher quantities, on average, than Medium and Low ones, in that order. Slander sessions then showed the opposite situation in which Low quality grades were the ones most produced, ahead of Medium and High ones, in that order. Finally, Medium quality grades were the most produced in Sybil sessions, with High and Low ones reaching similar averages. This shows that slander and Sybil treatments had a negative effect on the quality of products sold by vendors with slander operations leading to the production of Low quality products and Sybil operations Medium quality ones.

For this analysis, the number of products of each quality produced during each round were used instead of individual metrics as in the previous sections, as these data are categorical. This resulted in smaller sample sizes based on the combined number of rounds in all three groups (n = 90) rather than the number of products produced throughout sessions.

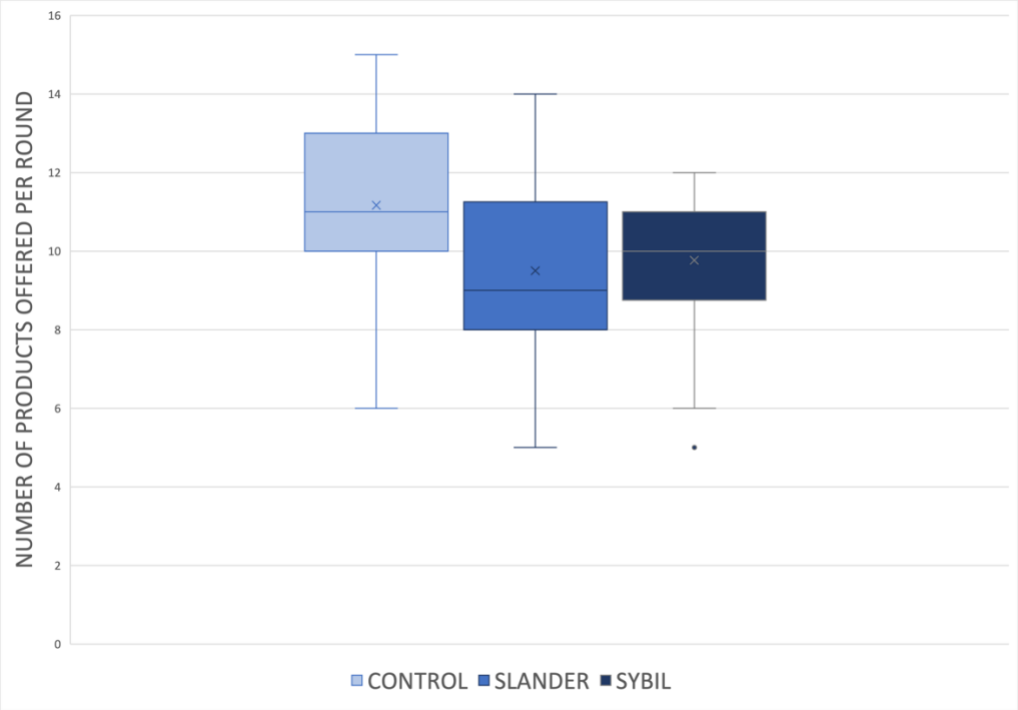


Figure 7.9: Boxplot for the High quality produced by vendors per round during the "market for lemons" game in Control, slander, and Sybil sessions

Overall, the number of High quality products offered by vendors was significantly affected by slander and Sybil interventions ($H(2)=10.3$, $p = 0.006$). Mann-Whitney U tests were conducted to follow-up on these findings. It appeared that significantly fewer High quality products were offered in the slander treatment (mean rank = 24.1) compared to those offered during the Control (mean rank = 36.9, $U = 258$, $p = 0.004$). Similarly, significantly fewer High quality products were offered in the Sybil treatment (mean rank = 24.8) compared to those offered during the Control (mean rank = 36.2, $U = 279$, $p = 0.01$). However, High quality products offered were not significantly different in the slander treatment (mean rank = 28.87) compared to those offered in the Sybil treatment (mean rank = 32.12, $U = 499$, $p = 0.463$). The null hypothesis of no difference is therefore rejected for two of the three groups.

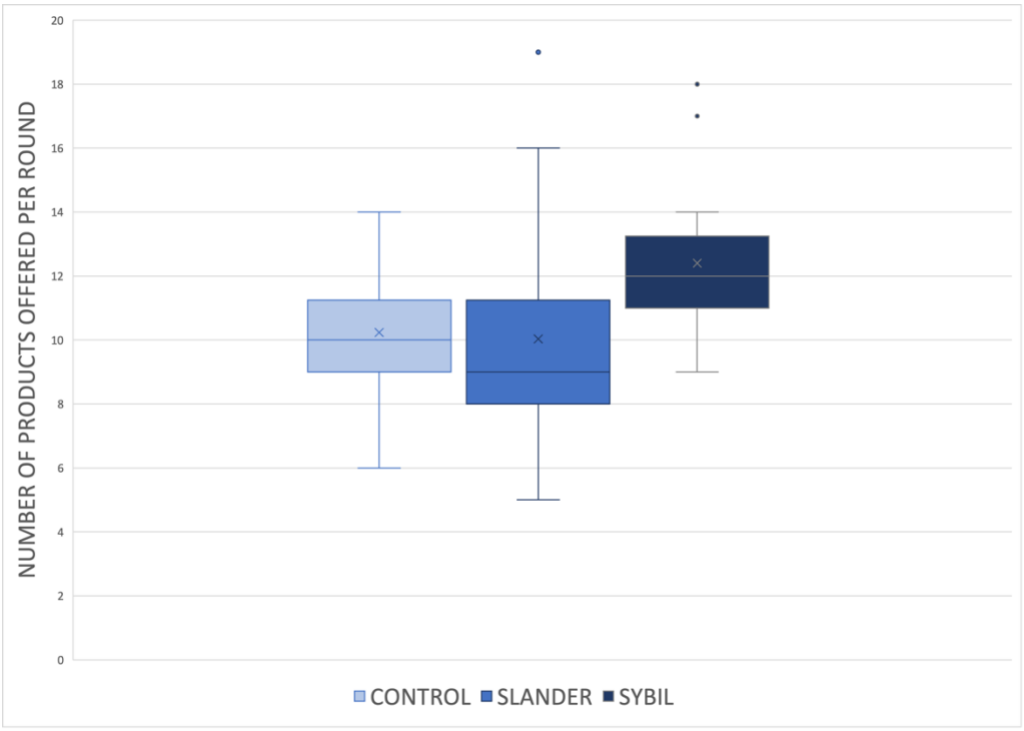


Figure 7.10: Boxplot for the Medium quality produced by vendors per round during the "market for lemons" game in Control, slander, and Sybil sessions

Overall, the number of Medium quality products offered by vendors was significantly affected by slander and Sybil interventions ($H(2)=19.5$, $p < 0.001$). Mann-Whitney U tests were conducted to follow-up on these findings. It appeared that Medium quality products offered were not significantly different in the slander treatment (mean rank = 28.15) compared to those in the Control (mean rank = 32.85, $U = 379.5$, $p = 0.293$). However, significantly more Medium quality products were offered in the Sybil treatment (mean rank = 38.95) compared to those offered during the Control (mean rank = 22.05, $U = 703.5$, $p < 0.001$). Similarly, significantly more Medium quality products were offered in the Sybil treatment (mean rank = 38.88) compared to those offered during the slander treatment (mean rank = 22.12, $U = 701.5$, $p < 0.001$). The null hypothesis of no difference is therefore rejected for two of the three groups.

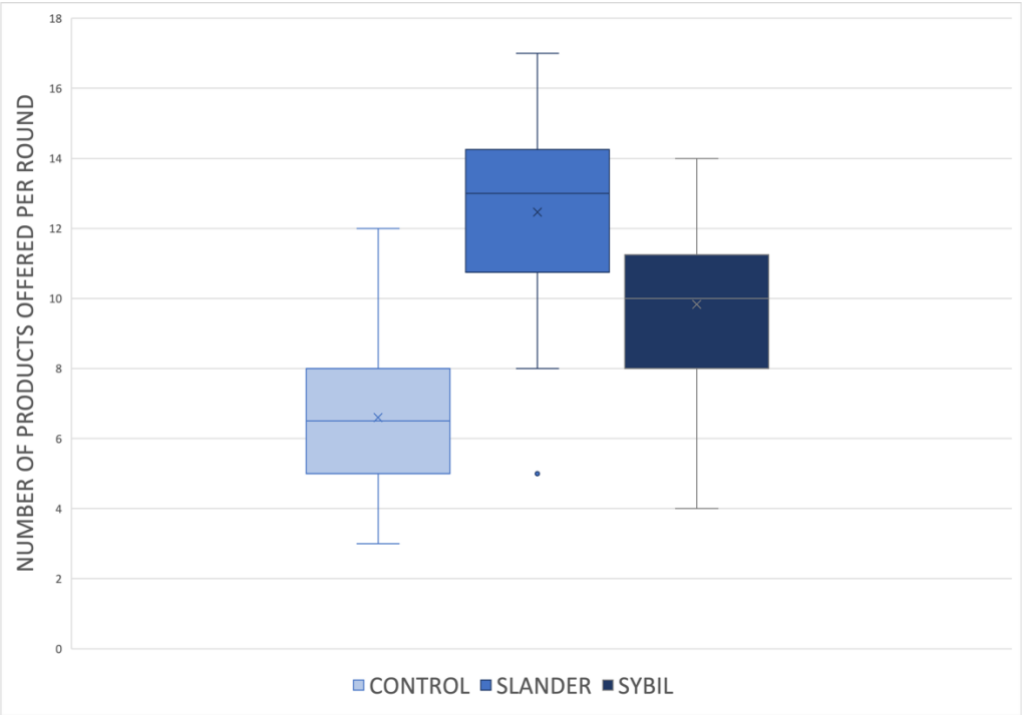


Figure 7.11: Boxplot for the Low quality produced by vendors per round during the "market for lemons" game in Control, slander, and Sybil sessions

Overall, the number of Low quality products offered by vendors was significantly affected by slander and Sybil interventions ($H(2)=50.6$, $p < 0.001$). Mann-Whitney U tests were conducted to follow-up on these findings. It appeared that significantly more Low quality products were offered in the slander treatment (mean rank = 44.08) compared to those offered during the Control (mean rank = 16.92, $U = 857.5$, $p < 0.001$). Similarly, significantly more Low quality products were offered in the Sybil treatment (mean rank = 41.97) compared to those offered during the Control (mean rank = 19.01, $U = 794$, $p < 0.001$). Finally, significantly more Low quality products were offered in the slander treatment (mean rank = 39.55) compared to those offered during the Sybil treatment (mean rank = 21.45, $U = 178.5$, $p < 0.001$). The null hypothesis of no difference is therefore rejected for all three groups.

There were clear changes in quality produced across experimental treatments, with vendors in each treatment producing a particular quality grade in higher proportions than the other two. These differences could stem from the fact that higher-quality products required larger investments from vendors, who weren't certain to be chosen by buyers for their purchase.

Lower investments in the way of cheaper Low and Medium quality production therefore appeared less risky but also maximised profits if these products were bought for high prices, although sometimes at the cost of vendors' reputations. However, given manipulations in sending and rating decisions, this was a calculated risk and one that would have been expected in the case of a "market for lemons" where quality is expected to reduce if it cannot be ascertained by buyers upon purchase.

The answer to research question 1.c. is therefore that slander and Sybil operations, in the case of this experiment, both had an impact on the quality of products offered by vendors, as shown by significant decreases in the amount of High quality products and increases in Low and Medium quality products compared to the Control sessions. Our third hypothesis that the product quality offered by cybercriminal vendors will decrease is therefore confirmed as both slander and Sybil operations decreased quality offered, to Low and Medium respectively.

7.2.4 Buying and sending decisions

Similar results were observed across treatments in terms of buying and sending decisions.

Table 7.3: Percentage of buying and sending decisions throughout rounds and across all treatments

	Control	Slander	Sybil
Sent	91	90	92.5
Not sent	8	9	7
Not bought	1	1	0.5

Similarly to quality produced in the previous section, the following analyses were based on the number of decisions not to buy and to default during each round, meaning the overall sample size remains the aggregation of all rounds for all three treatments (n=90).

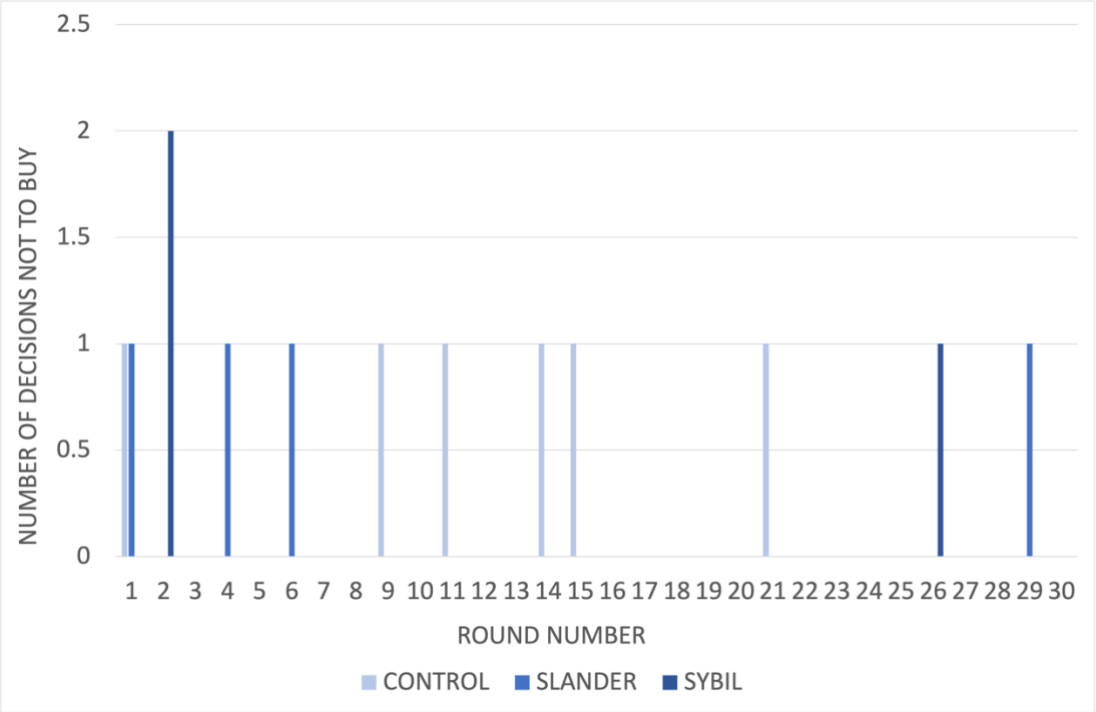


Figure 7.12: "Market for lemons" evolution of buyers' decisions not to buy throughout rounds and across treatments

Very few buyers chose not to buy from either vendor and these results were consistent across treatments. There were six rounds in the Control sessions when one buyer chose not to buy, four rounds in slander sessions, and two rounds in Sybil sessions, one of which included two buyers not buying. Throughout all rounds in these experiments, six products were not bought in the Control, four in slander sessions and three in Sybil sessions. Overall, the number of decisions not to buy was not significantly affected by slander and Sybil interventions ($H(2)=2.1$, $p = 0.353$), therefore no further tests were required and the null hypothesis of no difference could not be rejected.

Buying decisions therefore remained similar throughout rounds and treatments, with only very few buyers choosing not to buy products, due to them being able to make more money from buying a product of potentially Low quality instead of forfeiting their tokens at the end of the round, whether they trusted vendors in their trio or not. Decisions not to buy were mostly situated at the beginning of sessions and can therefore signal participants testing the system or making sense of the game. Additionally, a few participants decided not to buy later in the game with six of these 13 total decisions happening on or after Round 11, so this could

also reflect a loss of trust between participants. Indeed, Bolton et al. (2004) defined trust in their experiment as the percentage of products bought during each round. During this experiment, the majority of participants in all treatments still traded with participants they distrusted (see Appendix D.5) and buying percentages remained at 99% or above for all treatments. However, participants in the Control sessions were the ones who decided not to buy the most, so the interventions did not necessarily impact this metric.

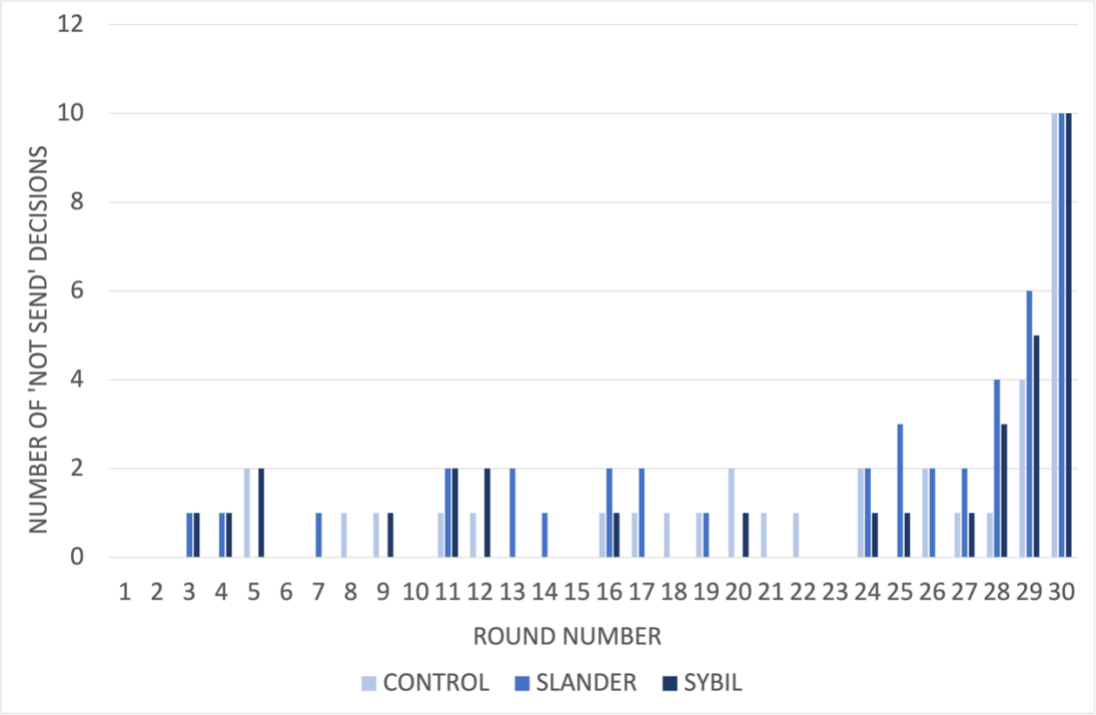


Figure 7.13: "Market for lemons" evolution of vendors' decisions not to send throughout rounds and across treatments

Vendors also seemed to consistently send their products, even in the Sybil treatment where not sending could have been construed as a 'compromised' decision, which could therefore have encouraged further defaulting. Only the last two experimental rounds in all sessions showed a sharp increase in decisions not to send, which is considered normal in these types of experiments as vendors try to maximise their payoffs when they no longer fear reputational consequences. In the Control sessions, 12 of the 30 rounds involved every vendor sending their purchases. In the remaining rounds, 12 rounds involved one vendor defaulting and four rounds two vendors, until the last two rounds when more than half of the vendors defaulted.

This therefore represented a 7 to 14% rate of default for the vendors whose products were chosen in these rounds, excluding the last two. In the slander treatment, 14 of the 30 rounds involved every vendor sending their purchases. In the remaining rounds, five rounds involved one vendor defaulting, seven rounds two vendors, one round three vendors, and one round four vendors, until the last two rounds when more than half of the vendors defaulted. The rate of default therefore ranged between 6 and 25% in these rounds, excluding the last two. In the Sybil treatment, 16 of the 30 rounds involved every vendor sending their purchases. In the remaining rounds, eight rounds involved one vendor defaulting, three rounds two vendors, and one round three vendors, until the last two rounds when more than half of the vendors defaulted. The rate of default therefore ranged between 6 and 19% in these rounds, excluding the last two. Although the Sybil treatment involved the 'compromise' of sending decisions, this therefore did not incentivise vendors not to send their products as participants in these sessions were the ones to send the most products to buyers.

Overall and throughout all rounds of these experiments, 33 products were not sent in the Control sessions, 42 in slander sessions, and 32 in Sybil sessions. The number of defaults was not significantly affected by slander and Sybil interventions ($H(2)=0.9$, $p = 0.634$), therefore no further tests were required and the null hypothesis of no difference could not be rejected.

Bolton et al. (2004) defined trustworthiness in their experiment as the percentage of shipping decisions during each round. Despite slight variations, neither intervention had a significant impact on the number of defaults, as more than 90% of products were sent across treatments and rounds, the slander treatment delineating the lower bound and the Sybil treatment the upper bound. It is surprising that participants in the Sybil sessions sent slightly more products than those in the Control treatment when adjusted for the number of participants in each session, despite the possibility during this treatment that 'not sending' could have been interpreted by buyers as a 'compromise' by the system. The reason for this lack of increase in defaults in the Sybil treatment would require further testing. Survey results confirmed that, overall, more than two thirds of all participants believed they exhibited trustworthy behaviour, as high as 75% and 80% for Sybil and Control participants respectively (although those numbers are still lower than the percentage of sending decisions). However, nearly 20% of slander participants admitted to not exhibiting trustworthy behaviour (see Appendix D.5).

The subjective rating mechanism, rather than the objective provision of historic behaviour in Bolton et al. (2004), was a new addition to "market for lemons" experiments and encouraged more than half of all participants to be more trustworthy, as high as 68% and 78% for Slander and Control participants respectively. However, nearly a quarter of slander participants were, to their own admission, not encouraged by that mechanism (see Appendix D.5).

The answer to research question 1.d. is therefore that both slander and Sybil operations, in the case of this experiment, did not have a significant impact on buying and sending decisions. Our fourth hypothesis that cybercriminal traders' decisions to buy and send products will decrease is therefore not confirmed as buying and sending decisions remained similar across treatments.

7.2.5 Trust

It is also important to examine whether the interventions had any impact on broader measures of trust. For this purpose, all the participants played the trust game before the "market for lemons" game, and then again afterwards.

Both trust games involved the same participants in order to test for differences following slander and Sybil interventions during the "market for lemons" game. The Kruskal-Wallis and Mann-Whitney U tests therefore do not suit this context. The non-parametric test for experiments including repeated measures (the same participants) and two conditions is the Wilcoxon Signed Rank test, the non-parametric equivalent of dependent t-tests. However, measures need to be matched to specific participants for each condition, which was not permitted by the raw trust game data. Therefore, no statistical tests are performed and only descriptive statistics are reported for trust game data.

During the Control sessions, the median number of tokens sent during the first and second trust games was 10 out of 25. However, the average number of tokens sent between both trust games decreased from 12.9 out of 25 to 11.7, therefore showing a slightly increase in lower amounts of tokens sent in the second game (see Figure 7.14). The median number of tokens sent back during the first trust game was 10, compared to 0 during the second. Indeed, although the amount of tokens sent back both before and after the "market for lemons" game was more likely to include 0 (see Figure 7.15), the amount of 0 tokens sent back during the second game greatly increased, showing a potential decrease in trust during the Control experiment.

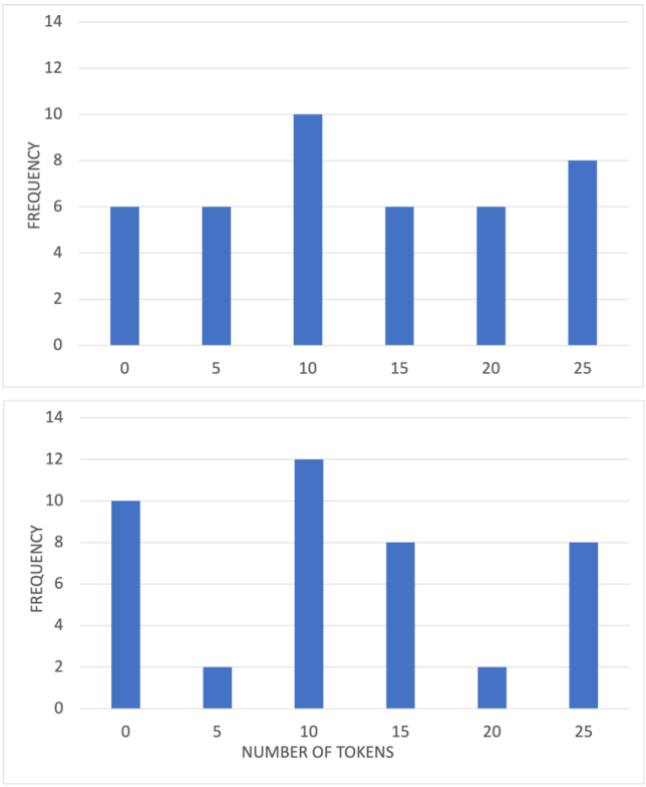


Figure 7.14: Frequency of tokens sent during the first (top) and second (bottom) trust games in Control sessions

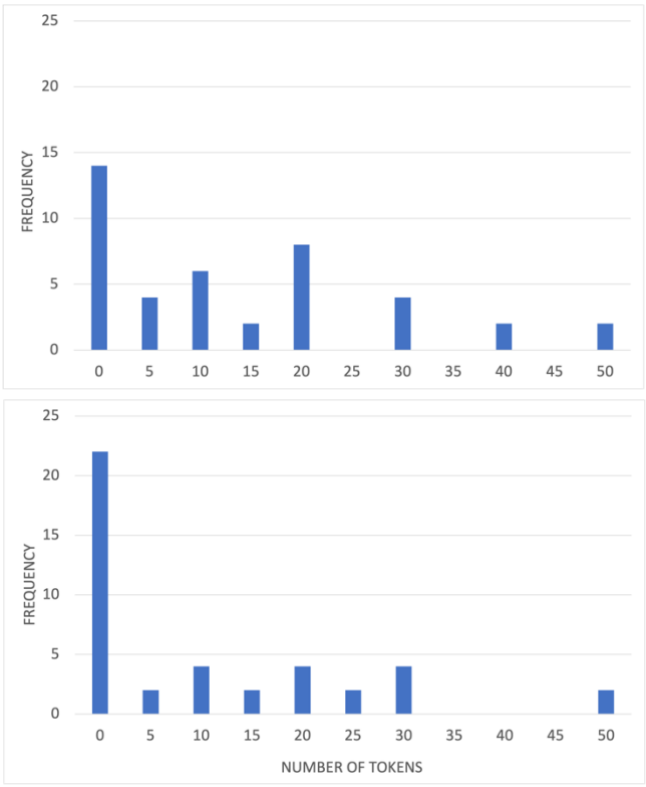


Figure 7.15: Frequency of tokens sent back during the first (top) and second (bottom) trust games in Control sessions

During slander sessions, the median number of tokens sent during the first trust game was 15 out of 25, compared to 12.5 during the second, a 17% decrease following the "market for lemons" game. Although a third of participants sent the maximum amount of tokens during the first game, that proportion decreased to only a quarter during the second game, in favour of smaller amounts (see Figure 7.16). The median number of tokens sent back during the first trust game was 10, compared to 5 during the second, a 50% decrease. Although the range of tokens sent back in the first game expanded from 0 to 40, this range decreased to 0 to 30 tokens during the second game (see Figure 7.17), showing a potential decrease in trust during the slander experiment.

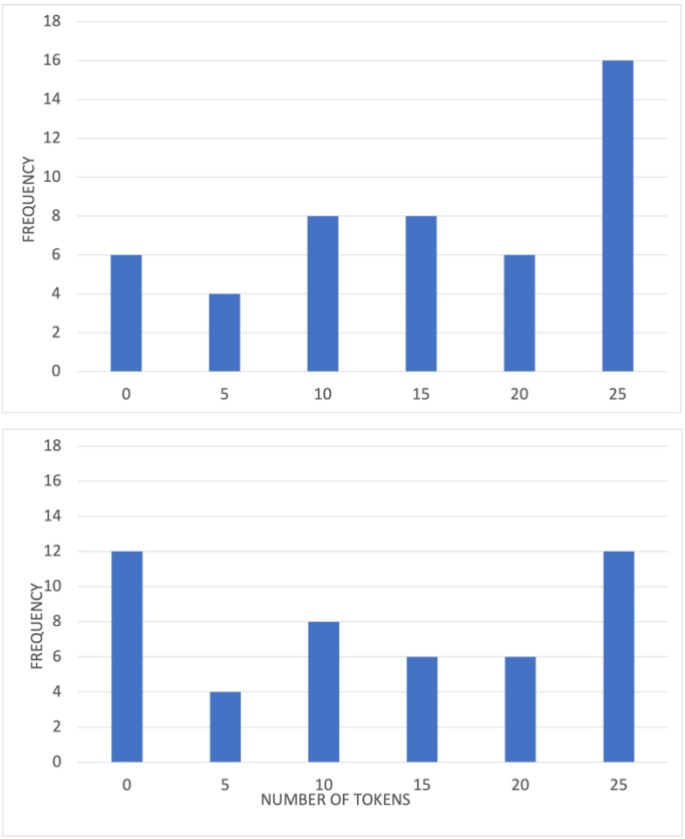


Figure 7.16: Frequency of tokens sent during the first (top) and second (bottom) trust games in slander sessions

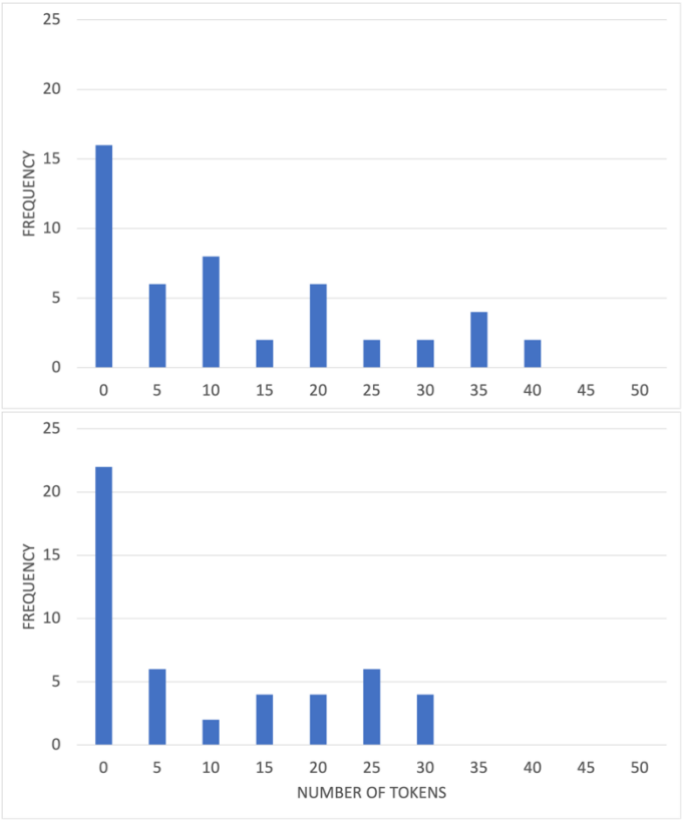


Figure 7.17: Frequency of tokens sent back during the first (top) and second (bottom) trust games in slander sessions

During Sybil sessions, the median number of tokens sent during the first trust game was 15 out of 25, compared to 10 during the second, a 33% decrease following the “market for lemons” game. Although the amount of 0 and 25 tokens sent during the first and second games remained similar, the second game involved more 5 and 10 token amounts compared to 15 and 20 tokens during the first game (see Figure 18). The median number of tokens sent back during the first and second trust games was 15. However, the average number of tokens sent back between both trust games increased from 13.5 out of 25 to 14, due to a slight increase in higher amounts of 20 and 35 tokens sent in the second game (see Figure 7.19).

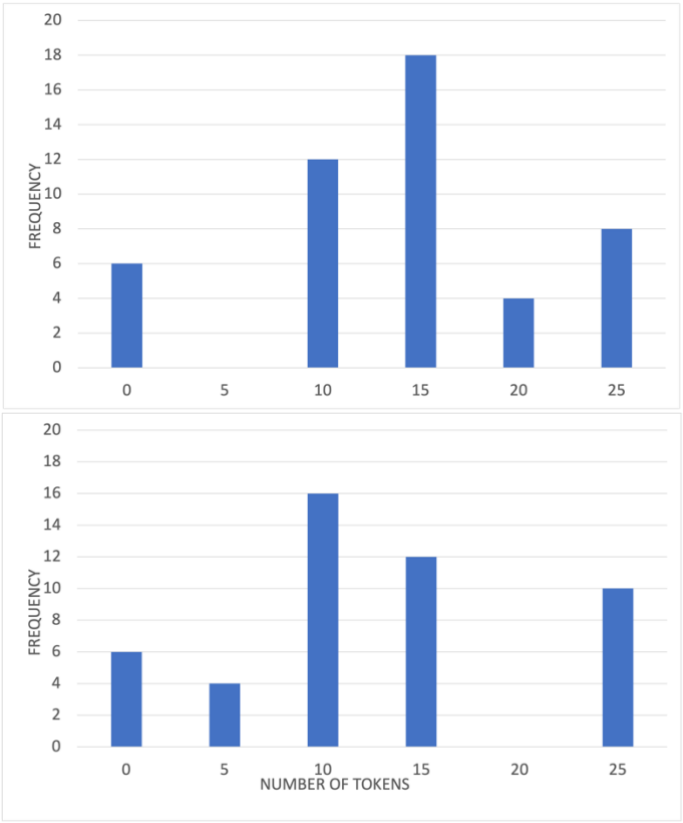


Figure 7.18: Frequency of tokens sent during the first (top) and second (bottom) trust games in Sybil sessions

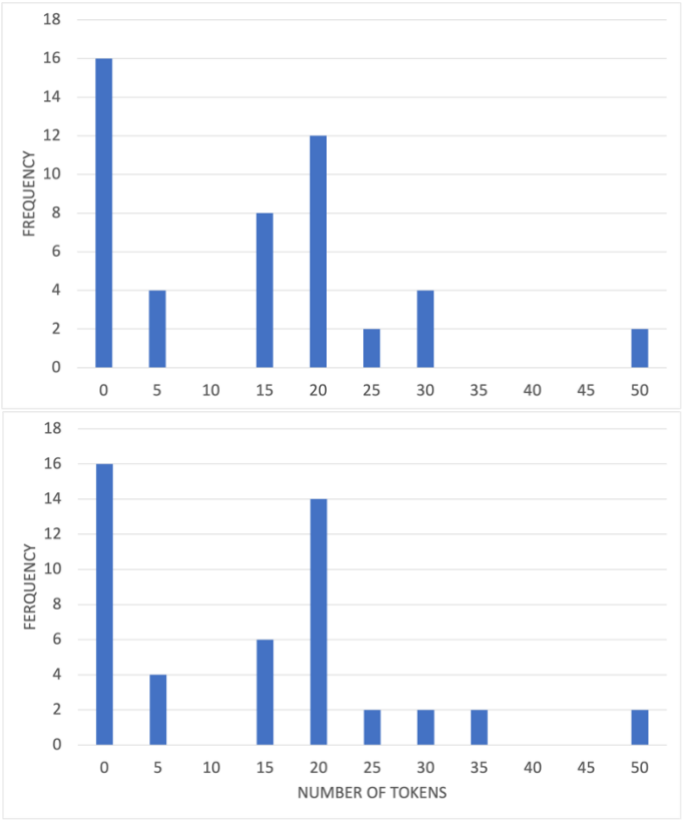


Figure 7.19: Frequency of tokens sent back during the first (top) and second (bottom) trust games in Sybil sessions

Overall, there were therefore slight decreases in the numbers of tokens sent and sent back after the "market for lemons" games, except for the final send back amounts in the Sybil treatment.

Trust games were used as a secondary game in order to measure any differences in trust levels at the beginning and at the end of the experiment. Results indicate that if trust levels diminished after the "market for lemons" game, they only did so very slightly.

According to participant survey data, more than 60% of Control and Slander participants disagreed that they got to know and trust the other participants they were trading with, compared to only 40% of disagreement within Sybil participants. Additionally, more than 50% of both Control and slander participants admitted to distrusting other participants compared to 33% of Sybil participants (see Appendix D.5). Beyond these participant differences, it could be further investigated whether this lack of decrease in trust could be due to empathy on the

part of buyers in the case of the Sybil interventions, as they understood that vendors in this treatment were not necessarily the ones to default but were also victims of the system, as are cybercriminal vendors when their products are intercepted by the Police or Customs.

The answer to research question 1.e. is therefore that slander and Sybil operations, in the case of this experiment, slightly decreased trust between participants. Our fifth hypothesis that trust between cybercriminal traders will decrease is therefore partly confirmed as slander and Sybil operations slightly decreased trust between participants and further testing could be performed on these metrics.

7.3 A new policing actor category

The findings presented overall paint a picture of a low-price and low-quality market, which supports some broader theories about "markets for lemons" and the importance of reputational mechanisms in online trade, as manipulating vendors' reputations deteriorated trade and trust. These findings are similar to those of Holt and Sherman (1999) following their own "market for lemons" experiment, where the experimenters observed a 'dramatic' decrease in price and quality as buyers were more inclined to buy low-priced products in situations of information asymmetry and at which price point it was only profitable for vendors to offer low-quality products. However, they are contrary to Akerlof's (1970) initial theory that vendors in "markets for lemons" are likely to offer lower-quality products and higher prices than they are worth to take advantage of the lack of information available to buyers, and therefore driving higher-quality and higher-priced products out of the market. In any case, these findings show that both slander and Sybil operations have an impact on cybercriminal traders' behaviours on these marketplaces.

> *"These are somehow communities and they are protected to a certain level because they are using Tor and encryption and anonymisation technologies, so in a way they are not completely dependent on trust because they can protect themselves. Nevertheless, if you are buying and selling you need to be able to trust the one you are buying from and hidden services do give the opportunity to build in that trust, you know, if you get ripped off by a vendor you can mention that and the vendors' image will go down or his status will go down, so there are mechanisms that are being used" (POI-D2)*

Coming back to the online illegal markets this experiment investigated, these results raise several questions about whether such low-price and low-quality markets would be a good measure of success for these policing operations, compared to taking down entire marketplaces and arresting users. This question needs to be answered from different perspectives. It is expected that low prices might encourage buyers to continue getting involved in these markets, as there might be less risk of 'loss of coin' (Bradley, 2019) if products are cheaper, potentially driving demand and trading volumes up for a time, until quality is seen to be sub-par or vendors default on their orders. Unlike other marketplaces

which might sell non-harmful products, this would therefore imply that a significant amount of harm could be caused by vendors offering low-price and low-quality drug, wildlife and other products, perhaps even greater than a market functioning optimally and offering safer products before disruption. From a Police standpoint of harm reduction and population protection, this strategy therefore does not seem ideal. However, such low-price and low-quality markets could also render these types of trades less profitable if only sold in small quantities.

> *"The reasons why these [markets] exist is because it's profit-driven. That's not the only part of it, but the career cybercriminals are doing it to make a living and where there is profit they will go looking for that. If by disrupting the cyber markets we can decrease profitability and increase their costs then it will reduce that burden of cybercriminality, and also make it a less lucrative opportunity for the next generation of young cybercriminals growing up, and so hopefully they will go elsewhere" (POI-D1)*

Knowing that cybercriminal vendors on these marketplaces are opportunistic and financially-motivated (POI-D4), this could be a good strategy to spur them to reduce their involvement with these trades, and one that seems more effective and long-term than other arrests and takedowns which have only had short-term effects. While some vendors will remain and are believed to be setting up their own single-vendor marketplaces in order to evade Police detection on larger marketplaces (Europol, 2019g), this tactic is only feasible for already-established and reputable vendors and will be more difficult to achieve for smaller and newer vendors. Some marketplaces will also put in place more technical processes in order to reduce the amount of trust traders need to put in one another and instead rely on processes such as blockchain, where transaction records are maintained across several computers linked in a peer-to-peer network. However, such systems will lead to the enforcement of premiums, which not every buyer will have access to and not every vendor will be invited to take part in. Larger audiences and smaller costs can be achieved through participating in trade through social media or instant messaging applications, which has seen a sharp increase in recent years (Babb, 2014; Thanki and Frederick, 2016; EMCDDA and Europol, 2019; Moyle et al.,

2019) and can accommodate traders who wish to remain more hidden than possible on Darknet markets (P-W2).

In response to our first research question in this chapter, both types of operations had an impact on cybercriminal traders' behaviours, encouraging vendors to offer lower prices and lower quality products, encouraging buyers to choose lower-priced products, and encouraging vendors to default on their orders, although these impacts were more pronounced in the case of slander interventions. These findings will need further testing to confirm how effective they could be in the real world and to ensure that practical tactics for their deployment are optimised.

These initial results therefore show that cybercriminal traders have played and could continue to play a prominent role in the decrease in profitability and the overall policing of their own marketplaces, as their behaviours are replicated at scale by Police, moral crusaders, and others, and trade is forced to stop or relocate. Consequently, the answer to our second research question is that cybercriminal traders have indeed unintentionally participated in the policing of their own marketplaces and should therefore be included in policing classifications, as shown by the cyber policing classification devised in the following Discussion chapter.

7.4 Conclusion

This chapter presented the pilot results of a social laboratory experiment replicating a "market for lemons" where buyers don't possess any information about the quality of products and services for sale or about the intentions of vendors. This experiment allowed the researcher to observe participants' behaviours and decision-making when policing interventions were conducted, which is challenging to ascertain on real Darknet markets, as well as gauging these operations' effectiveness at reducing trust, and therefore trade, based on these results.

This chapter was divided in three parts: the first part described previous market experiments and the specific focus of this experiment on slander and Sybil operations as a way to answer this thesis research questions; the second part then detailed the consequences of slander and Sybil interventions on prices offered, purchase prices, quality offered, buying and sending decisions, and trust between experiment participants; and finally the third part argued that cybercriminal traders should be considered policing participants in the online illegal trade policing context.

In the case of this experiment, both slander and Sybil tactics proved effective in making the marketplace one of low-price and low-quality, although slander tactics reached sharper results. Targeting marketplaces' reputational mechanisms, therefore suggests that these interventions may render cybercriminal trade less profitable for administrators and vendors and less efficient for buyers. This confirms the hypothesis that cybercriminal traders are responsible at least partly for the policing of their own marketplaces. Such an impact gives rise to a new category of policing according to which cybercriminal traders themselves have disrupted trust on their own marketplaces and assisted the rest of the policing ecosystem by providing them with knowledge and tools to undermine trust on a larger scale. However, this new category differs from the knowledge and tools cybercriminals have given to the Police knowingly, in the way of informing or whistleblowing. This chapter argues that cybercriminal traders unintentionally, through their behaviours and choices, have provided the Police and private organisations with new policing tactics.

These are only initial experimental results, however, so they should be treated as suggestive and tested further. In order to be more robust, reliable, and generalisable, this experiment would need to be replicated with larger sample sizes and online instead of in the laboratory to create more realistic conditions. Although the aim of this pilot experiment was simplicity, the experiment could be enhanced in the future by adding features such as 1) conducting both slander and Sybil operations simultaneously in order to observe their combined effect, 2) different volumes of trade, 3) different proportions of policing interventions to test their relative impact on market forces and trust levels until a potential tipping point is identified past which trust cannot be recovered, 4) informing participants about the criminal nature of the marketplace and assigning roles based on buyers' and vendors' different motivations and therefore ensuring a certain volume of defaults, 5) compromising all or 95% of ratings to 5 stars to more closely resemble ratings given on Darknet markets, or 6) strategically choosing which ratings or sending decisions to compromise based on participants' payoffs, to confirm the precise circumstances in which self-serving cybercriminal traders are most disruptive. Similar experiments not focussed on cybercriminal traders but the wider ecosystem could also be carried out by 'arresting' cybercriminal traders in the marketplace or by taking down a marketplace and witnessing potential displacement to another. Beyond the laboratory, there is also scope for these operations to be tested by the Police and other agencies in real Darknet markets, as part of field experiments, as was discussed by some private organisations (POI-W6). In any case, the adaptation of experimental methods to cybercrime and cybercriminal trade specifically offers an exciting research opportunity going forward.

Beyond the Police, legal online platforms, and private organisations directly involved in the policing of online illegal drug and wildlife trades, cybercriminals themselves have therefore had an indirect role to play in this policing. The following Discussion chapter summarises the contribution of each of these actors in the policing of online illegal drug and wildlife trades. These findings are then collated in a new cyber policing classification and the first policing script detailing who is involved, in what way, and at what stage of the policing process.

8 Discussion

In the second to last chapter of this thesis, insights from the four previous empirical chapters are brought together to evaluate the role each actor is playing in the policing of online illegal drug and wildlife trades, how they complement each other, when, and where they each participate in the policing timeline. Based on these insights, the researcher suggests practical policy recommendations about complementary tasks in this arena.

Building on the four groups involved in the policing of online illegal drug and wildlife trades, this thesis designs a new cyber policing classification. Indeed, Button (2019)'s policing classification is argued not to fit the context of online illegal drug and wildlife trades policing. This new classification, however, is more broadly applicable to other types of cybercrimes, which are only partially covered in Button (2019)'s framework. This thesis also introduces the concept of and produces the first 'policing script', an adaptation of crime scripts used to describe the conduct of crimes and their various stages, to identify where the Police and others could intervene most effectively and create connections with other actors in the policing ecosystem. Providing such insights about the most effective actions each actor can take therefore aims to outline what each organisation and sector could and should rely on others for, as they are best-placed and most-skilled to perform these actions. Such scripts will ideally encourage them to move past their potential pre-conceived notions about one another and allow for more effective and complementary policing in the future.

This Discussion chapter is divided in four parts, each one summarising findings from the four previous empirical chapters and answering one overall thesis research question: the first part examines the actors involved in the policing of online illegal drug and wildlife trades, designs its own classification of cyber policing involving all of these actors and assesses the extent to which Button (2019)'s policing classification fits this context; the second part then ties together the activities performed by each of these policing actors; the third part devises a policing script presenting all of the previous insights in a novel way and uses it to compare the policing of online illegal drug and wildlife trades; and the fourth part recommends actions to be taken and collaborations to be generated for these types of policing to become more effective in the future.

8.1 Who is involved in the policing of online illegal drug and wildlife trades?

In order to answer this thesis' first research question, the first section of this Discussion chapter integrates findings from the previous four empirical chapters to ascertain which groups are involved in the policing of online illegal drug and wildlife trades. Once these groups are described and their broad characteristics identified, they are each categorised as a part of the researcher's cyber policing classification.

8.1.1 The Police

Despite their prominent role in the policing of online illegal drug and wildlife trades, the previous findings concluded that the Police's involvement in the former has been taking precedence over the latter, not only in the number and range of operations they perform, but also in the amount and length of their discourse about policing. One of the reasons for this is likely that the security onus for the latter has been put on online marketplaces which facilitate wildlife trade, instead of illegal marketplaces such as Darknet markets and online pharmacies which facilitate drug trade, and which must be dealt with by the Police. However, the Police maintain relationships with other policing groups, as argued by Button (2019), despite some issues of trust between groups who work in different sectors and might therefore not fully understand others' skills and motivations in this space. While the Police might have denied the existence and input of other groups at first, growingly and begrudgingly recognised their value, and competed with them to ascertain their control, the experts interviewed for this thesis all emphasised the importance of public-private partnerships as part of their roles, whether they were policing drugs or wildlife. Building that trust in partnerships is therefore paramount to the effectiveness of these policing activities (Bures, 2013). That collaborative aspect of policing described by Button (2019) therefore applies in these two cases. Although the Police clearly stand the closest to Button (2019)'s State and Hybrid Policing categories, which not only encompass general agencies such as the London Metropolitan Police, but also specialised agencies such as the National Crime Agency, no distinction is made in this thesis between these two categories. Instead, the Police in all of their forms, specialisms, and geographical levels are argued to represent one category of policing provided by the State. This category is called 'statutory policing' as it is required by statute and is expected by the

public in both product realms. Despite its prominent role, statutory policing depends on many other private policing actors for its success.

8.1.2 Legal online platforms

Legal online platforms are also an important part of the online illegal drug and wildlife trades policing apparatus. Indeed, they have published trade policies for their users to abide by, and monitor their platforms, as staffed services would a physical location. They have also put in place security processes such as the automatic detection of certain keywords for review, and have the power and authority to take action on the relevant listings and users.

Button (2019)'s Private Security Industry category appears like the closest fit for online platforms in this context. While Button and George's (2000) definition of the Private Security Industry starts broad, it is then narrowed down to organisations focussing on security, and therefore does not fully apply to legal platforms.

> *"The term 'private security industry' is a generic term used to describe an amalgam of distinct industries and professions bound together by a number of functions, including crime prevention, order maintenance, loss reduction, and protection […] To be included within the industry, personnel must have primarily a security role" (George and Button, 2000)*

Indeed, legal platforms were not initially created with security as their focus, instead placing trade or social connections at their core. However, this thesis has shown that a large volume of illegal trade, specifically that of drugs and wildlife, does occur on legal platforms, requiring them to put more emphasis on security, which they have done in accordance with the steps laid out in George and Button (2000)'s definition. The scope of Button (2019)'s Private Security Industry category is therefore too narrow in this context. Indeed, legal platforms, despite only bearing a secondary focus (at best) on security, are in fact an essential part of the private policing apparatus in this context, not only ensuring their in-house security but also providing security as a service to their users during trading activities. These legal platforms are referred to as 'requisite policing' in this classification because new technological circumstances, regulations, and societal changes have made it necessary for them to

participate in this type of policing. However, several security-centred private organisations have been participating in this policing voluntarily.

8.1.3 Private organisations and individuals

While several of the organisations included in the private aspect of this policing are security companies, providing threat intelligence services for a fee and therefore theoretically fitting within George and Button (2000)'s Private Security Industry definition, they do not in fact provide security services related to online illegal drug or wildlife trades. Instead, private organisations such as these protect their clients from threats including information and financial thefts or Denial of Service attacks based on the activity they observe on the Darknet and elsewhere. They are therefore very far removed from drugs and wildlife. However, specifically in the case of drugs, while gathering information relevant to their clients, these organisations come across activity related to drug trade and witness the evolution of the Darknet ecosystem. They are therefore able to share this information on a voluntary basis with the Police and the wider public, although it is not directly within their work remit. Similarly, not-for-profit organisations involved in raising awareness and reducing demand for drugs and wildlife are not acting on behalf of clients or for a fee, instead they are advancing their cause following interest from the public to address these issues. Unlike other organisations participating in the policing of online illegal drug or wildlife trades more incidentally, these groups possess specific expertise on drug and wildlife matters, which the Police and legal online platforms do not necessarily have, and which they need to provide them with on a voluntary basis, as they have not been commissioned to perform such work. The associations which have emerged and involve organisations from various industries and sectors coming together to support one another in these efforts are also voluntary in nature. There is therefore a place for several groups to come together in a polycentric manner, following years of specific groups taking the lead (Dupont, 2016b) and an emphasis on specific actors contributing their specialised skills or preferential position in the system (Cherney et al., 2006).

Despite being security-minded private organisations and groups of individuals, they do not fit within Button (2019)'s Private Security Industry category, as they perform the above activities voluntarily. These organisations do not necessarily suit his Voluntary Policing category either,

however, as this focusses on groups and individuals directly supporting the Police on a formal or informal basis in very limited contexts such as search parties (Button, 2019). Organisations and individuals in the private, public, non-profit, and academic sectors therefore make up a new private policing category for this type of policing, 'volitional policing'. Indeed, they willingly use their specialised resources and knowledge to support the Police and legal platforms in their interventions, while not being required or remunerated to do so and not focussing on specific issues important to and signposted by the Police. A final category of actors has also had an impact unwillingly.

8.1.4 Cybercriminal traders

Finally, cybercriminal traders emerged as a category of interest upon understanding the impact they have had on the policing of their own marketplaces. Indeed, not only have traders reduced trust on their own marketplaces, by scamming and exit scamming one another, therefore undermining the reputational infrastructure put in place by administrators, but doing so has also led the previous three categories of policing to perform new and related interventions. In light of some of the criticism more direct operations have received over the last few years, including the short-term consequences of arrests and takedowns as various forms of displacement are available to traders (Van Buskirk et al., 2014; Décary-Hétu and Giommoni, 2016; Bradley and Stringhini, 2019), attacking human relations rather than technical infrastructure opened a new avenue for policing. While such 'insider knowledge' could be compared to information given by cybercriminal traders about their associates and activities in exchange for lighter sentences (Poulsen, 2011; Dupont, 2016c), or the whistleblowing of cybercriminal traders against others who are still allowed to trade while they aren't (LP-W1; Krebs, 2015), this thesis argues that such an exchange is done voluntarily (and therefore encompassed in the volitional policing category). Indeed, in these cases cybercriminals know they are giving information to the Police and what might ensue. In the case of this new 'unintentional policing' category, however, the scamming and exit scamming behaviours exhibited by cybercriminal traders is not knowingly performed to share information with the Police. Instead, the Police have been gathering and replicating such behaviours against cybercriminal traders' will and better judgment. Such a category of actors who, unbeknownst to them, were helping shape policing strategy is not reflected in Button

(2019)'s or previous classifications, yet it is one that clearly has a place in the policing of online illegal drug and wildlife trades.

The previous categories of actors involved in the policing of online illegal drug and wildlife trades are summarised in a new and more relevant classification in this context. These categories form the basis of the cyber policing classification whose broader categories below are argued to perform the activities outlined in the following section of this chapter.

Table 8.1: The cyber policing classification

Category of policing	Examples
Statutory Policing **Policing provided by the State for its citizens in all of its forms, as required by statute and expected by the public**	Metropolitan Police Service (UK) National Crime Agency (UK) Europol United Nations Office for Drugs and Crime World Customs Organisation
Requisite Policing **Organisations and individuals whose participation in policing has been rendered necessary by technological, regulatory, and societal changes, although it is not their specialism**	Trading and auction websites (e.g. eBay) Social media platforms (e.g. Facebook) Instant messaging applications (e.g. WhatsApp)
Volitional Policing **Policing by private organisations and individuals performed of their own volition, as their work sometimes differs from their policing input and they are not necessarily remunerated for it**	Centre for Safe Internet Pharmacies Cyjax Flashpoint International Fund for Animal Welfare Wildlife Justice Commission
Unintentional Policing **Policing that stems from cybercriminal behaviours which unintentionally disrupt trust and cybercriminal activities from the inside and give the Police and others new ways to police their crimes**	Cybercriminal traders Darknet market administrators

Although this classification was based on the online illegal drug and wildlife trades policing case studies, the categories created from the specific actors in these cases are expected to apply in other cyber policing contexts.

Indeed, statutory policing is provided for other types of cybercrimes and entire policing units have been created to focus on cyber security issues at regional, national, and international levels. As their websites become increasingly informative and contain the ability to report these types of crimes, the Police aim to position themselves as the first port of call for victims of cybercrimes.

In a recent report about the evolution of law enforcement action in the age of technology, Europol (2021b) also affirmed that "profiteers in cyberspace have to be involved in safety and security". Private organisations acting online have therefore been required to participate in policing by complying with statutory police investigations, even if security is not their specialism. As such Europol has been working with a range of private partners in the technology, financial, and communication industries (Europol, 2021d). One of its partners, Microsoft, has been involved in the policing of botnets alongside the Police (Dupont et al., 2017). The corporation's Digital Crimes Unit focusses on business email compromise, malware, ransomware, and tech support fraud (Microsoft, 2021) which take place on their Operating Systems.

The volitional actors in the case of online illegal drug and wildlife trades mentioned passing information they came across to the Police when it involved child sexual exploitation materials (POI-D4) or terrorist activities (POI-D5). Requisite actors can also support other types of cybercriminal investigations on a voluntary basis, such as Microsoft designing new technology to detect and disrupt instances of online child exploitation (Microsoft, 2021). Additionally, spammers inform against one another (Krebs, 2015) in the same way cybercriminals do when they are blocked from certain trading platforms (LP-W1) or when they prevent competing Darknet markets from staying online through Denial of Service attacks (EMCDDA & Europol, 2017a; Europol, 2019f, 2019g, 2020e; UNODC, 2018c).

Finally, cybercriminals make unintentional mistakes that lead to the Police gathering information and taking action against them. For instance, Dread Pirate Roberts was linked to

an email address registered to Ross Ulbricht during the Silk Road investigation (Bilton, 2018). Hackers also sometimes post comments in forums infiltrated by enforcement personnel asking questions about security measures taken by the US Department of Defence before mounting a malware attack on one of its locations (Lin, 2016), therefore allowing for attribution and further action. Additionally, more than 800 cybercriminals were arrested in June 2021 following their use of the FBI-created ANOM encrypted platform. ANOM offered features other platforms didn't, which enticed criminals to switch to using their services. The platform then intercepted millions of users' messages about their criminal activities for 18 months preceding the arrests, not all of which were related to trade (Europol, 2021a).

While the exact details of how these four categories of actors participating in policing activities varies, these four groups are therefore argued to be present for a range of cybercrimes. This cyber policing classification could therefore be further investigated and refined for other types of cybercrimes.

8.1.5 Policing leads

Beyond the type of policing actors involved in the policing of online illegal drug and wildlife trades, this thesis also pointed to the Police taking the lead on online illegal drug trade policing, while legal platforms and private organisations and individuals led the policing of online illegal wildlife trade, with cybercriminal traders being peripheral in both cases. This is an important distinction that wasn't included in Button (2019)'s classification, as it assumed the State and Hybrid Police are widely protecting the State while the Private Security Industry protects individuals and organisations in exchange for a fee. As well as a public and private policing dichotomy, there therefore should also exist a public and private *leading* dichotomy, because every crime is not dealt with to the same degree by the same agencies, despite what their labels might suggest. This does not mean, however, that the other groups aren't involved, as this thesis demonstrated public and private involvement in the policing of both types of trades and the need for such partnerships. Indeed, private organisations in this sphere have different priorities and expertise and therefore require support from the Police, and vice versa. These differences are particularly noticeable in the policing of online illegal drug and wildlife trades, and it is likely they also apply to other types of policing. To honour these differences, distinctions are made in the policing script devised in the third section of

this Discussion, between actors and activities that differ in the policing of online illegal drug and wildlife trades.

The answer to this thesis' first research question is therefore that the Police, legal platforms, private organisations and individuals, and cybercriminal traders are all involved in the policing of online illegal drug and wildlife trades. These actors have formed the basis for new cyber policing categories: statutory policing, requisite policing, volitional policing, and unintentional policing. Indeed, Button (2019)'s policing classification is too narrow to consider the range of actors and motivations involved in the policing of online illegal drug and wildlife trades, and it does not mention the unintentional impact of cybercriminal traders on their own marketplaces. Additionally, while all of these groups are represented in the policing of both online illegal drug and wildlife trades, some are more involved in one than in the other.

The activities performed by the above actors in these two types of policing are discussed in the next section.

8.2 What activities do these policing actors perform?

In order to answer this thesis' second research question, the second section of this Discussion chapter integrates findings from the previous four empirical chapters to ascertain what activities the Police, legal online platforms, private organisations and individuals, and cybercriminal traders perform to disrupt online illegal drug and wildlife trades. Indeed, several academic studies have stopped at identifying who participates in policing activities (Button, 2019; Moshier et al., 2019), but not what they do beyond the arrest, seizure, takedown, and content removal labels. In a field as opaque as cybercrime, understanding these activities is therefore paramount to increasing the efficiency of this process.

Following expert interviews, content analysis, and a social laboratory experiment, these activities have been divided into four main stages – 1) monitoring, 2) sharing, 3) policing interventions, and 4) reporting – each of which is detailed in turn below.

8.2.1 Monitoring

The first stage of policing for two of the actors described in the previous section – legal online platforms and private organisations and individuals – is monitoring.

Prior to any monitoring, laws and policies have to be put in place that require abidance by the public. In the case of online illegal drug and wildlife trades, this can take the form of national or international legislation banning the sourcing, manufacturing, trading, and usage of certain products and that of policies prohibiting the sale of certain products on individual legal sites. While this does also hold true for Darknet markets which sometimes ban the trade of specific products on their marketplaces (Flashpoint, 2017a; Cyjax, 2018c; Martin et al., 2018a), these policies are more prominent on surface web platforms which publish trade policies with the support of private organisations and individuals to ensure the legitimacy of their sites. Following this, legal platforms and their administrators specifically, have been held responsible for monitoring their sites, which they do both manually and automatically, to detect potential illegality for further action (LP-W1). Organisations and individuals in private, non-profit, and academic organisations have also gathered information on these sites, assisting them in monitoring the vast and constantly increasing amount of content they host. While private organisations and individuals are not responsible for this monitoring in the

same way that legal platforms are, they want to better understand these trades and disrupt them in support of their clients or cause. In addition to these sites, private organisations and individuals have also monitored Darknet markets in order to support the Police in their endeavours, due to the large volume of content to sift through on these marketplaces. This confirms that everyone from the Police to big corporations and lone citizens "*has their role to play*" in the policing of online illegal trade (POI-D1). The Internet, as well as providing various opportunities for criminals to communicate, manage, organise, promote, and market their activities online (Lavorgna, 2014a, 2014b), has therefore also offered new opportunities for monitoring and investigation (Lavorgna, 2016), not only available to the Police but also to others in the wider policing sphere.

These insights are then shared between policing groups in order to create a broader picture of the threat and to increase the effectiveness of policing activities.

8.2.2 Sharing

The second stage of policing for three policing actors – the Police, legal online platforms, and private organisations and individuals – is sharing, which itself happens in different stages.

Following their individual monitoring, private organisations and individuals first report any criminal findings to legal platforms and the Police for further action. If needed, as well as sharing this information, private organisations and individuals can also share expertise with these two groups, as they support them in improving their own monitoring processes or understanding how best to disrupt these trades. If this sharing was done with legal platforms, they will then move on to take further action, as described in the following stage. If this sharing was done with the Police, additional monitoring and sharing steps will ensue, as agencies dig further into the issues reported, gathering their own information into specific marketplaces, products, and people, given their additional powers of investigation. If illegal content was reported on legal platforms, the Police are also entitled to explicitly ask for additional data to be given to them. Additionally, the Police can then share this and other information with other enforcement agencies around the world, or ask them for information, to assist them on their own territories or perform collaborative operations. These staged

back-and-forths between all three groups ensure that the Police and legal online platforms have all the information necessary to intervene.

The information and expertise shared between groups then lead to direct policing interventions on Darknet markets and legal online platforms.

8.2.3 Policing interventions

The third stage of policing for three policing actors – the Police, legal online platforms, and cybercriminal traders – is direct policing interventions, which take many forms.

As explored in this thesis' Literature review chapter, policing is a term broader than the Police, as it involves various stakeholders beyond those employed by the State (Brodeur, 2010). As such, many groups can be seen to perform their own versions of policing interventions following monitoring and sharing stages. The Police, however, still hold a prominent place in the policing of online illegal drug trade specifically, as it occurs on the Darknet, which cannot be disrupted as authoritatively by others alone. The Police, upon obtaining the necessary information and collaborating with the necessary groups, have therefore arrested cybercriminal traders and administrators, seized illegal products, and taken down entire Darknet market infrastructures and networks. While these activities are reactive, the Police have also performed more proactive operations, such as prevention and trust disruption. For the former, agencies have been created which remind Internet users acting in grey areas of what is legal and what isn't, and the harms they expose themselves to by taking part in illegal activities online. For the latter, the Police have learnt from the interventions cybercriminal traders themselves have performed, scamming buyers and exit scamming entire marketplaces, which have disrupted trust and trade unintentionally. Slander and Sybil operations have therefore been conducted by the Police (P-D2), and will be used by others who have obtained ethical approval (POI-W6), to decrease trust on these marketplaces, in the hope of creating longer-term decreases in profit and trade. Alongside these interventions on the Darknet, legal platforms have also removed illegal content and blocked criminal users they or others identified on their marketplaces to ensure their legitimacy.

The successes accomplished during these interventions are then reported to inform one another and the wider public.

8.2.4 Reporting

The fourth stage of policing for three policing actors – the Police, legal online platforms, and private organisations and individuals – is reporting on their and others' interventions.

After the conduct of policing interventions, relevant successes are reported to different groups and the wider public. Before reporting can take place, as legal action is sometimes required, the Police collaborate with the prosecution to bring charges to cybercriminal traders and administrators. The consequences of specific operations are then analysed in order identify relevant numbers, trends, and any changes in the aftermath of these interventions, so they can be shared. The Police release news articles specific to each intervention, detailing who participated, when, what actions they took, and what the consequences were, assuming this information is not confidential. The main points of these articles are then often summarised and included in quarterly or yearly publications focussing on specific areas of enforcement and showcasing the work of specific agencies. Similar interventions are also reported on by legal platforms and private organisations and individuals on their blogs and websites, to keep their following, clients, and the wider public informed about recent policing activities. However, covert operations, such as slander and Sybil attacks, and ongoing operations (unless they are instigated by cybercriminals themselves and put users in danger) are understandably not reported on by the Police to preserve their discretion. More information may be found in non-profit organisations' reporting than others, however, as their continued funding and survival depends on the quantity and quality of their work. Based on these interventions, their volume, and degree of success, some legal platforms, and private organisations and individuals then lobby lawmakers to implement tighter controls on these trades and ensure more similar operations are performed in the future. Finally, the Police, legal online platforms, and private organisations and individuals raise awareness about the state of policing in this sphere, trends, convictions, seizures, takedowns, and the ecosystem more widely. Awareness has been raised in various ways and to various degrees, from social media posts to reports published by several organisations, and the involvement of the wider public to share these messages is paramount.

The answer to this thesis' second research question is therefore that there are four main activities involved in the policing of online illegal drug and wildlife trades – 1) monitoring, 2) sharing, 3) policing interventions, and 4) reporting – which are each performed by a subset of the overall policing actors identified in the previous section. While the specifics of these activities sometimes differ between the policing of both types of trades, the details of which are explored in the following section, the broad activity categories and their chronology remain common to both.

The above activities described for the policing of online illegal drug and wildlife trades are now summarised and matched to their respective actors in a policing script.

8.3 How similar or different are the policing actors and activities involved in the policing of online illegal drug and wildlife trades?

After summarising this thesis' findings with regards to the actors and activities involved in the policing of online illegal drug and wildlife trades, and in order to answer this thesis' third research question, the differences between these two types of trades are highlighted through a policing script.

The policing script presented below aims to mirror crime scripts used to better understand the sequence of events involved in committing crimes (Sugiura et al., 2012) in order to identify offenders' modus operandi and the criminal opportunities they are exploiting (Lavorgna, 2013). Ultimately, these scripts inform at what stages criminal processes might be most effectively prevented or disrupted (Lavorgna, 2018). Although crime scripts were initially devised with regards to offline crime, a common example including the theft of cars (Cornish, 1994), they have also been applied to online crimes where they are deemed particularly insightful to uncover cybercriminal actions undertaken behind the scenes (Warren et al., 2017). Indeed, Leukfeldt et al. (2016b) identified different types of cybercrimes depending on the level of technology used and amount of interaction with victims when performing attacks on online banking, for instance. They argue that all the relevant crime scripts involved similar steps in the formation these cybercriminal networks, from forming a core group of cybercriminals, to contacting other criminal enablers, identifying victims, capturing their information, and transferring funds to money mules. However, the specific activities they performed to conduct their chosen attacks varied depending on the extent to which they relied on technology and/or on human interactions (*Ibid*.). More closely related to the cybercrimes investigated for this thesis, Hutchings and Holt (2015) devised the first crime script detailing the people and steps involved in online data theft and monetisation, including but not limited to sellers, buyers, suppliers, and moderators who installed software, chose their marketplace(s), created their profile, learnt the rules to abide by on their platform(s), exchanged information, and currency. Lavorgna (2014a, 2014b) has also specifically applied such crime scripts to online illegal drug and wildlife trades, including the poaching, smuggling, transport, purchase, and distribution steps reviewed earlier in this thesis. These scripts therefore show that there exist both online and offline components to these trades

(Lavorgna, 2014a, 2014b); they are complex crimes that are difficult to script in their entirety as they involve many stakeholders and steps (Moreto and Clarke, 2013), as does their policing.

Previous crime script sequences have been described in a number of ways, including specific functions such as preparation, entry, pre-condition, mental actualisation, doing, post-conduction and exit (Cornish, 1994). However, the more precise these sequences, the less they apply to the other side of the script – policing. Consecutive stages of activity adapted from Lavorgna's (2013; 2014a, 2014b) crime script framework were therefore used to convey the chronological aspect of these activities with simplicity, following the Preparation, Pre-Activity, Activity, and Post-Activity model, as this categorisation is broader and also applies in this case. Despite being closely scrutinised alongside crime scripts in this section, as they are the scripts that spurred the idea for policing scripts, the script produced as part of this thesis is entirely original. Indeed, no previous crime has been examined through the lens of the policing actors or activities involved in their disruption, as done in this thesis. Focus was instead put on the offenders committing these crimes. However, online illegal trade policing is complex and encompasses many stakeholders and steps detailed in previous sections, so summarising all of the information about who should participate in this policing, when, and how in a concise script is necessary to increase the effectiveness of this policing in the future. This novel concept in the field of sociology and (cyber)criminology also aims to provide practical insights about which actors are involved and which activities are performed at various stages of the policing process, so various stakeholders can more easily collaborate with one another. Indeed, this script will ideally encourage current policing actors to lean on one another to perform the tasks they are best suited for, and others to take part in similar activities if they are interested and able to get involved in this type of policing. Some actors might even perform different and complementary activities which are not yet part of the script if they have the skill and ability necessary to increase the efficiency of the process.

It should be noted this policing script is tentative, as it is based on a limited sample size of interviews, publications, and experimental sessions for the two crimes under investigation (Chiu et al., 2011), and should therefore be refined as more insights are gathered. Additionally, he proposed policing script focusses on the actors and activities involved in the policing of the online components of these trades, some of which could have an incidence on

offline demand, supply, and policing. However, this script does not imply offline policing components do not exist in this case, these were merely outside the scope of this thesis. Policing actors could therefore complete this script with additional offline stages they or others are involved in.

The policing script is presented in the form of a table below, including a different column for each policing group and a different line for each policing activity. As most of the actors and activities are similar between online illegal drug and wildlife trades policing, they are presented in the same table. However, distinctions are made for individual actors and activities where these differ between both types of trades.

Table 8.2: Online illegal drug and wildlife trades policing script

Stage of policing	Policing activity	The Police	Legal online platforms	Organisations and individuals	Cybercriminal traders
Stage 1: **Monitoring** **(Preparation)**	1.1 Create rules of conduct	Participate in the writing of rules and laws following insights on the ground	Write and publish platform trade policies with private organisations and individuals <u>Drugs:</u> Policies on average are concise and use mostly passive and negative language to discourage illegal trade <u>Wildlife:</u> Policies on average are lengthy, including many different keywords, use passive and negative language, and signpost additional information about relevant legislation	Support legal platforms to draft trade policies for their sites	
	1.2 Gather information		On own platform	On Darknet markets, surface websites, social media sites, instant messaging applications	
	1.3 Analyse information		Identify recent trends and criminals on own platform	Identify recent trends and criminals on Darknet, surface websites, social media sites, instant messaging applications	

Stage of policing	Policing activity	The Police	Legal online platforms	Organisations and individuals	Cybercriminal traders
Stage 2: **Sharing** **(Pre-activity)**	2.1 Share information			With the Police for further action With legal online platforms for site updates and action	
	2.2 Share expertise			With the Police for specific situations and wildlife products With legal online platforms for policy publication and crime detection	
	2.3 Gather further information	Following private organisations' and individuals' insights, dig deeper into specific illegal marketplaces and criminals	Following Police's and private organisations' and individuals' requests, dig deeper into specific users and listings		
	2.4 Share further information	With other Police forces around the world	With Police following requests for platform data		
	2.5 Share further expertise	Between specialised drugs and wildlife units and general units			
	2.6 Prepare for policing interventions	Select illegal marketplace, trader Familiarise with site practices Get trust of relevant users and relevant infrastructure access Get support from other agencies	Select listing, trader	Select legal platform, trader	Select marketplace, trader Familiarise with site practices Get trust of relevant users

Stage of policing	Policing activity	The Police	Legal online platforms	Organisations and individuals	Cybercriminal traders
Stage 3: **Policing interventions** **(Activity)**	3.1 Perform direct interventions on platforms, traders, trade	<u>Drugs:</u> Arrest cybercriminal traders and administrators Take down illegal marketplaces on Darknet and surface web (e.g. online pharmacies) Disrupt networks Seize illegal products Observe cybercriminal traders' behaviours on the marketplaces and replicate them (e.g. slander and Sybil attacks) <u>Wildlife:</u> Seize illegal products Take down illegal markets on surface web	Remove illegal content on site Block criminal users from site		Scams Exit scams

Stage of policing	Policing activity	The Police	Legal online platforms	Organisations and individuals	Cybercriminal traders
Stage 4: **Reporting** **(Post-activity)**	4.1 Pursue legal action	Collaborate with prosecution and experts to bring case to court			
	4.2 Analyse consequences	Keep track of new markets, new users, new listings Quantify results	Keep track of new traders, new listings on own platform Quantify results	Keep track of new platforms, new users, new listings Quantify results	
	4.3 Report on intervention	News posts about recent operations on agency website and wider reports about progress on specific issues	News articles about wider ecosystem operations, rarely mentioning own interventions	Blog posts and reports about ecosystem, sometimes mentioning own involvement	
	4.4 Lobby		Police and policymakers for tighter laws and controls	Police and policymakers for tighter laws and controls	
	4.5 Raise awareness	<u>Drugs:</u> News articles about recent successes Reports about specific drug-related themes <u>Wildlife:</u> News articles about recent successes	Blog posts about specific themes and current happenings in the ecosystem	<u>Drugs:</u> Blog posts about current happenings in the ecosystem Reports about specific drug-related themes Short anti-trade messages on social media <u>Wildlife:</u> Blog posts about recent successes Reports about dangers associated with wildlife trade Short anti-trade messages on social media	

The answer to this thesis' third research question is therefore that the actors and activities involved in the policing of online illegal drug and wildlife trades are mostly similar between drugs and wildlife and only differ for a few steps. These differing steps include the content and formulation of trade policies on legal platforms, which differ in their content and length, the interventions conducted by the Police due to the location of these trades, and the format and content of different reporting about the policing of these two types of trades.

Building on the above policing script, the final section of this discussion provides practical insights to increase the effectiveness of online illegal drug and wildlife trades policing in the future.

8.4 How can these types of policing be rendered more effective in the future?

Considering the growing amounts of online illegal trade and in order to answer this thesis' fourth research question, practical insights are now shared in order to render these policing activities more effective in the future.

8.4.1 Policing actors

This thesis has identified a breadth of actors involved in the policing of online illegal drug and wildlife trades, including statutory policing, requisite policing, volitional policing, and unintentional policing actors. This classification greatly expands upon Button (2019)'s framework and categories. However, this list is not assumed to be exhaustive. Indeed, while specific actors were identified through interviews with experts participating in this policing as part of various organisations and positions, it is expected many more in the fields of finance and transport specifically are also involved between the requisite and volitional policing categories, but are more secretive.

The range of organisations and sectors represented demonstrates that everyone really has a role to play in this kind of policing, even if they appear far-removed from drug and wildlife trades. This thesis therefore advocates for more actors to support already-existing policing actors and conduct their own activities in this space with the guidance of the policing script, which suggests stages were support is needed and even signals what missing stages could be filled.

8.4.2 Monitoring

The monitoring stage of policing is a crucial one that involves many actors one might not intuitively associate with this activity. However, the support private organisations and individuals have provided in this realm, from devising online trade policies to setting up monitoring procedures and actively scouring the Internet, should continue to be sought by the Police and legal online platforms as part of their manual and automated monitoring activities. In fact, such support could even be expanded, if resources permit, as private organisations and individuals could test legal platforms' monitoring processes and evaluate their progress, as highlighted by a legal platform administrator who asked a non-profit

organisation to run a test on their site and report the amount of potentially illegal listings (LP-W1). A year later and upon conducting another test, the organisation reported seeing fewer illegal listings on the site, showing clear signs of improved monitoring (LP-W1). While this was not the aim of the organisation conducting these tests, it was invaluable for the administrator to evaluate the effectiveness of their platform monitoring, and such services could be offered more widely to support the development of these processes. As such, departments in existing organisations or new organisations could be set up to perform these checks or even outsource the monitoring process. Indeed, by hiring the monitoring services of experts, legal platforms would not have to spend time training their own employees to perform this monitoring, but they could instead rely on organisations whose expertise and interests already lie in these issues. Such organisations would then be more closely related to Button (2019)'s Private Security Industry category, as they would be focussed on the security of these platforms, ensuring the legitimacy of the listings on their behalf, and leaving legal platform administrators to focus on the core of their activity.

8.4.3 Sharing

This thesis has demonstrated the importance of information and expertise sharing when policing online illegal drug and wildlife trades. As suggested earlier in this section, more collaborations could be set up and made explicit to the public, so other actors can observe there are legitimate and impactful support networks in this arena that they could also benefit from. Making these collaborations visible and reporting on their results might not only help increase trust different policing actors put in one another as part of these operations, but also increase the effectiveness of future policing interventions as more information is shared and broader pictures of these crimes can be drawn for further action.

Such information and expertise sharing, in some circumstances, have been facilitated by organisations such as the Coalition to End Wildlife Trafficking Online and the Center for Safe Internet Pharmacies, which bring together different actors and encourage them to support one another. As these groups have grown since their establishment, the benefits of such associations are clearly being recognised and will hopefully continue to inspire others to get involved. While the size and expertise of these organisations can be an advantage for global legal platforms requiring their support, as homogenous trading policies can be implemented

and several case studies can help refine the systems in place, similar regional groups might also help in these efforts. Indeed, products such as drugs and wildlife are highly regulated internationally, but there also exist various national and regional differences to these regulations. While international platforms such as eBay and Google can benefit from the support of international associations, smaller national platforms might feel more comfortable getting involved in similar associations closer to home. Indeed, these organisations might better understand their market and relevant legislation, while remaining connected to the pioneering associations their support model is based upon.

8.4.4 Policing interventions

Due to the range of policing actors involved in the policing of online illegal drug and wildlife trades and their specific expertise and motivations for participating in this policing, they cannot all be involved in all of the policing interventions listed. Priorities for products to focus on and interventions to conduct have therefore been drawn by all actors. Indeed, this thesis showed the Police focus on drugs over wildlife and on the Darknet over the surface web, for instance. However, it is important support continues to be given to private organisations and individuals and legal platforms performing their own interventions, as the powers and authority of the Police are often needed to drive operations forward. In line with the previous trend of creating more collaborations to monitor trade and share information, cross-sector collaboration should also be leveraged during interventions themselves, where possible.

Additionally, in order to take full advantage of cybercriminal traders' insights into the policing of their own platforms, more research could be undertaken and more focus placed on trust-based disruption operations, such as slander and Sybil operations on the Darknet. Indeed, infrastructure-based disruption operations have been criticised in the past for their short-term results and the opportunities they provide for cybercriminal traders and administrators to improve their platforms and become more resilient to these attacks. More emphasis should therefore be placed on the human aspect of these disruptions, as technologies such as blockchain can only replace human trust to a certain extent, and these relationships will still be required to some degree on these platforms (POI-D2).

8.4.5 Reporting

The various types of publication formats and contents shared by the above actors have shown just how many approaches there are to reporting on policing activities. Different actors reported on different interventions in different ways. While previous interventions were the ones most talked about by the Police, private organisations emphasised the interventions they participated in, explained the theory behind these operations, and pointed to scams currently in progress to protect users. Although ongoing operations should not be shared with the public, more policing actors should follow the Police's lead and report on previous interventions. There are legitimate reasons for which legal platforms and private organisations might not want to report on interventions they were involved in or performed themselves, however, raising awareness about the Police's interventions would increase availability bias for cybercriminal traders and administrators. Constantly reading about Police interventions on online illegal trade would emphasise the fact that these disruptions happen frequently and that the entire policing apparatus is involved in them. By the same token, the Police should aim to report further on the policing of online illegal wildlife trade, as the quantity and length of articles currently available on that topic is limited. This would show cybercriminal traders that they are addressing the issue, and that legal online platforms and private organisations are not the only ones taking action. Indeed, the Police and their additional power and authority have more impact on the cybercriminal community, as shown by the relocation of the online drug trade on the Darknet, as the perceived risk of apprehension is greater than for the trade of wildlife.

This project's focus on two similar yet different case studies allowed for precise and actionable insights to emerge for future policy developments in the realm of online illegal drug and wildlife trades policing, as presented in this final section. Such insights could also be valuable for other policing spheres were similar actors and activities might be involved in policing and benefit from policing scripts to assess the current situation and devise new strategies.

The answer to this thesis' fourth research question is therefore that there are still many ways to increase the effectiveness of online illegal drug and wildlife trades policing. Many of these strategies are centred around further collaboration and links between actors in various sectors in order to support one another and bring new perspectives to this arena, as "it takes a network to defeat a network" (IFAW, 2018a).

8.5 Conclusion

The findings from the four empirical previous chapters were brought together and summarised in this Discussion chapter through the creation of a new cyber policing classification and the first policing script.

Overall, these findings show that Button's (2019) policing framework does not entirely apply in the context of online illegal drug and wildlife trades and a new classification of cyber policing is therefore required to encompass all of the actors involved in this type of policing. Additionally, the novel policing script presented in this Discussion chapter did not only enable the advancement of sociology and (cyber)criminology knowledge by providing a complementary concept to that of crime scripts, but it also provided practical insights about the actors and activities involved in the policing of online illegal drug and wildlife trades. Indeed, the script should help different groups to rely on one another for different activities and other actors to enter this space upon understanding where they might be most impactful in the future. Specific recommendations were also provided stemming from this script and related to each actor and activity involved.

This Discussion chapter was divided in four parts, each one summarising findings from the four previous chapters and answering one research question: the first part analysed the actors involved in the policing of online illegal drug and wildlife trades, designed its own classification of cyber policing involving all of these actors, and assessed the extent to which Button (2019)'s policing framework fits this context; the second part then tied together the activities performed by each of these policing actors; the third part devised a policing script presenting all of the previous insights in a novel way and used it to compare the policing of online illegal drug and wildlife trades; and the fourth part recommended actions to be taken and collaborations to be generated for these types of policing to become more effective in the future.

The final chapter of this thesis will draw conclusions about the answers obtained through this research and the contribution of these findings to the sociology and (cyber)criminology fields.

9 Conclusion

This concluding chapter aims to summarise the answers obtained as part of this research and the contribution of this thesis to the fields of sociology and (cyber)criminology.

This thesis addressed a simple problem, the rise of online illegal drug and wildlife trades with all the harms and challenges they engender, and the lack of integrated information about who is policing these trades and how. This problem is an important one to tackle to increase the effectiveness of the policing of these trades, especially in light of the COVID-19 pandemic which has exacerbated these challenges.

Previous academic literature was first analysed, including sociology, (cyber)criminology, and economic theoretical perspectives. While the increase in online illegal drug and wildlife trades on the Dark and surface webs was mentioned in both academia and industry, among other products and services traded in this way, few insights were uncovered about the policing of these trades. Wider theories of crime and policing therefore had to be sought in relation to other types of trades and cybercrimes. Indeed, while Police interventions in the way of arrests and takedowns were often mentioned in relation to online illegal trade, much of which involves drugs, the support they have received from other organisations and individuals and the consequences their interventions have had were rarely mentioned. One of these theories, the most applicable to this thesis as it was recently updated to include technological aspects, was that of Button (2019) who defined four main actors, both public and private, involved in general policing activities: 1) the State Police, 2) Hybrid Police, 3) Voluntary Policing, and 4) Private Security Industry. These policing categories were therefore evaluated in light of the illegal trades under review for this thesis, as they threaten our environment, health, and security, and many challenges seem to prevent their effective policing. Due to this thesis' interdisciplinary nature and its focus lying at the intersection of different academic literatures, the concepts and theories encompassed in the initial review were wide-ranging. However, none fully addressed the challenges this thesis aimed to tackle, as each one only provided a small, targeted piece of the puzzle. This research therefore took inspiration from these disciplines and combined their research methods and insights to advance knowledge on this specific topic not only theoretically but also practically. Indeed, only by understanding who

and what is currently involved as part of these interventions and how various actors can come together will we improve this process, which was the aim of this thesis.

As such, this thesis answered the questions:

1. Who is involved in the policing of online illegal drug and wildlife trades?
2. What activities do these policing actors perform?
3. How similar or different are the policing actors and activities involved in the policing of online illegal drug and wildlife trades?
4. How can these types of policing be rendered more effective in the future?

To answer these questions, this thesis used mixed social science methods to gather complementary insights as part of this exploratory project. First, the researcher conducted 20 semi-structured interviews with experts working for the Police, private, non-profit, and academic organisations, which allowed for a better understanding of different groups' roles in the policing of online illegal drug and wildlife trades. Then, the researcher used content analysis to gather quantitative data about the frequency of specific expressions mentioned in 200 Police and other publications, which also allowed for more qualitative insights to be drawn about the policing operations referenced by certain organisations at specific times. Finally, the researcher conducted a social laboratory experiment, which enabled the simulation of a fictious online marketplace where 138 participants' behaviours could be observed in response to specific policing interventions. Each of these methods came with its strengths and limitations. Interviews allowed for experts to share their stories, but these were limited to English-speaking experts around the world and only applied to their own circumstances rather than being universal experiences. Content analysis gathered a lot of previously unexamined data which was curated to be as complete and representative of the categories of interest as possible, but only focussed on written communications at the expense of audio and visual ones which are more sparsely available. The social laboratory experiment involved a steep learning curve and reached basic results which need to be further tested, but it involved the use of experiments in a new field and led to a better understanding of the roles criminals play in policing. Ultimately, all of these methods were great learning experiences and allowed for the gathering of complementary qualitative and quantitative data that formed the basis of this thesis cyber policing classification and policing script.

The contribution of this thesis to the fields of sociology and (cyber)criminology is two-fold, as this thesis devised both 1) a new cyber policing classification of the actors and activities involved in the policing of online illegal drug and wildlife trades, and 2) the first 'policing script' that complements existing crime scripts used to better understand these types of crimes and that improves our understanding of their policing with the aim of increasing the effectiveness of this process.

This thesis argues that there are four main types of actors involved in the policing of online illegal drug and wildlife trades – 1) the Police, 2) legal online platforms, 3) private organisations and individuals, and 4) cybercriminal traders. These actors form the basis of broader categories in a new cyber policing classification involving: 1) statutory policing, 2) requisite policing, 3) volitional policing, and 4) unintentional policing. While some of these categories are in line with Button (2019)'s assessment of policing in the digital age, his framework does not entirely suit this context. Indeed, the categories he devised are too narrow to consider the range of actors and motivations involved in the policing of online illegal drug and wildlife trades, and he does not mention the unintentional impact of cybercriminal traders on their own marketplaces. This thesis also demonstrated that actors perform a range of policing activities to disrupt online illegal drug and wildlife trades, including 1) monitoring, 2), sharing, 3) policing interventions, and 4) reporting, with different actors being involved during each of these stages. A policing script was then devised to integrate these detailed analyses, compare practices between drug and wildlife policing, and provide more insights to individual policing actors about their own and others' contribution to this type of policing. This thesis therefore has wider implications than the academic community, not only providing novel theoretical frameworks to be tested and used in the wider cyber context, but also sharing practical insights about the work performed by various policing stakeholders. As collaboration was a recurring theme in interviews and content analysis, the script specifically will ideally encourage these policing actors to act more collaboratively by signalling who is best-placed and most-skilled to get involved at different stages in the policing process and increase the effectiveness of this process in the future. Policy recommendations are provided to that effect to ensure every policing actor and policing activity is informed by others' best practices, resources, and skills.

The findings and conclusions from this thesis can not only be used to refine our understanding of the policing of online illegal drug and wildlife trades and the various actors and activities it involves, but also to model the complex policing of other types of crimes, such as other cybercrimes mentioned in the Discussion chapter and other financial and trafficking crimes which involve various stakeholders across sectors, industries, and countries. Further research could therefore be undertaken about the policing of these crimes using the cyber policing classification and policing script to increase our understanding of the actors and stages involved and ultimately increase their effectiveness. The practical insights and recommendations offered in summary of these findings can also be applied by practitioners in the Police and other public and private organisations to identify potential collaborators for their policing activities and encourage others to participate in this multi-faceted policing.

These policy recommendations include 1) further collaboration between the Police and other policing groups both directly and indirectly working in the online trade and security spheres, 2) continued and extended support from private organisations and individuals in devising trade policies, detection mechanisms, and monitoring their effectiveness, as key players within this policing sphere, 3) the creation of local and regional associations bringing various policing organisations together and supporting the Police and legal platforms with the legislation and issues in their specific regions, 4) collaborative and human-centred policing interventions, and 5) more reporting on policing activities, even in broad terms, in order to show the Police and other organisations are actively policing these trades and cybercriminal traders will not continue to engage in these crimes with impunity.

Further research could also be conducted into other types of online illegal trades which have become more prominent on the Darknet and social media, such as firearms, personal and financial information, and human trafficking. Future research could involve testing the cyber policing classification applies to these types or trades, devising distinct 'policing scripts' for them, and encouraging the involvement of additional individuals and organisations in their policing. Such research could be conducted using the same research methods as this thesis, potentially involving other types of interviewees and content to analyse, or using different methods altogether. These studies and scripts will then enable us to police these harmful trades more effectively, thereby protecting our environment, health, and security.

References

Adams, J. (1965). Inequity in Social Exchange. *Advances in Experimental Social Psychology, 2*, 267.

Aldridge, J., & Decary-Hetu, D. (2014). Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. *SSRN Electronic Journal*. doi:10.2139/ssrn.2436643

Altheide, D. L., & Schneider, C. J. (2013). *Qualitative media analysis* (2nd ed.). Thousand Oaks, Calif. ; London: SAGE Publications.

Arechar, A. A., Dreber, A., Fudenberg, D., & Rand, D. G. (2017). "I'm just a soul whose intentions are good": The role of communication in noisy repeated games. *Games and Economic Behavior, 104*, 726-743. doi:10.1016/j.geb.2017.06.013

Attrill-Smith, A., Fullwood, C., Keep, M., Kuss, D. J., Holt, T. J., & Lee, J. R. (2019). *The Oxford Handbook of Cyberpsychology* (1 ed.): Oxford University Press.

Ba, S. (2001). Establishing online trust through a community responsibility system. *Decision Support Systems, 31*(3), 323-336. doi:10.1016/S0167-9236(00)00144-5

Ba, S., & Pavlou, P. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly, 26*(3), 243-268. doi:10.2307/4132332

Ba, S., Whinston, A. B., & Zhang, H. (2003). Building trust in online auction markets through an economic incentive mechanism. *Decision Support Systems, 35*(3), 273-286. doi:10.1016/S0167-9236(02)00074-X

Babb, F. (2014). Instagram has a drug problem. Retrieved from https://venturebeat.com/2014/09/19/instagram-has-a-drug-problem/. [March 31st 2020]

Babbie, E. R. (2016). *The practice of social research* (Fourteenth ed.). Boston, MA: Cengage Learning.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2013). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction, 109*(5), 774-783. doi:10.1111/add.12470

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy, 35*, 24-31. doi:10.1016/j.drugpo.2016.04.019

Bartlett, J. (2014). *The dark net*. London: Cornerstone Digital.

Becker, H. S. (1963). *Outsiders : studies in the sociology of deviance*. New York : London: Free Press ; Collier Macmillan.

Belleflamme, P., & Peitz, M. (2018). Inside the engine room of digital platforms: Reviews, ratings, and recommendations. *IDEAS Working Paper Series from RePEc*.

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open, 2*(C), 8-14.

Benn, S. I., & Gaus, G. F. (1983). The public and private: concepts and action. In S. I. Benn & G. F. Gaus (Eds.), *Public and private in social life* (pp. 183-221). London: Groom Helm.

Bereby-Meyer, Y., & Roth, A. E. (2006). The Speed of Learning in Noisy Games: Partial Reinforcement and the Sustainability of Cooperation. *American Economic Review, 96*(4), 1029-1042. doi:10.1257/aer.96.4.1029

Berelson, B. (1952). *Content analysis in communication research*. Glencoe, Ill: Free Press.

Berg, J., Dickhaut, J., & McCabe, K. (1995). Trust, Reciprocity, and Social History. *Games and Economic Behavior, 10*(1), 122-142. doi:10.1006/game.1995.1027

Bergman, M. K. (2001). White Paper: The Deep Web: Surfacing Hidden Value. *The Journal of Electronic Publishing, 7*(1). doi:10.3998/3336451.0007.104

Bhaskar, V., Linacre, R., & Machin, S. (2019). The economic functioning of online drugs markets. *Journal of Economic Behavior and Organization, 159*, 426-441. doi:10.1016/j.jebo.2017.07.022

Bhattacharjee, R., & Goel, A. (2005). Proceedings of the 2005 ACM SIGCOMM workshop on economics of peer-to-peer systems. In (pp. 133-137).

Bilton, N. (2018). *American kingpin : catching the billion-dollar baron of the Dark Web*. London: Virgin Books.

Bolton, G., Katok, E., & Ockenfels, A. (2004). How Effective Are Electronic Reputation Mechanisms? An Experimental Investigation. *Management Science, 50*(11), 1587-1602. doi:10.1287/mnsc.1030.0199

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *An Interdisciplinary Journal, 67*(3), 265-288. doi:10.1007/s10611-016-9653-3

Bouchard, M. (2007). On the Resilience of Illegal Drug Markets. *Global Crime, 8*(4), 325-344. doi:10.1080/17440570701739702

Bradley, C. (2019). On the Resilience of the Dark Net Market Ecosystem to Law Enforcement Intervention. In G. Stringhini & H. Borrion (Eds.). Crime and Security Science: UCL (University College London).

Bradley, C., & Stringhini, G. (2019). *A Qualitative Evaluation of Two Different Law Enforcement Approaches on Dark Net Markets*. Paper presented at the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).

Brewer, M., & Crano, W. (2014). Research design and issues of validity. In H. Reis & C. Judd (Eds.), *Handbook of research methods in social and personality psychology* (pp. 11-26). Cambridge: Cambridge University Press.

Brewer, R. (2014). *Policing the waterfront : networks, partnerships, and the governance of port security*. Oxford: Oxford University Press.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management, 29*(3), 408-433. doi:10.1108/13639510610684674

Brodeur, J.-P. (2010). *The policing web*. Oxford: Oxford University Press.

Broseus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Decary-Hetu, D. (2016). Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Sci Int, 264*, 7-14. doi:10.1016/j.forsciint.2016.02.045

Broseus, J., Rhumorbarbe, D., Morelato, M., Staehli, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic Sci Int, 277*, 88-102. doi:10.1016/j.forsciint.2017.05.021

Brown, D. C., & Iles, S. (1985). *Community constables : a study of a policing initiative*. London: Home Office.

Bryman, A. (2012). *Social research methods* (4th ed.). Oxford: Oxford University Press.

Bures, O. (2013). Public-private partnerships in the fight against terrorism? *An Interdisciplinary Journal, 60*(4), 429-455. doi:10.1007/s10611-013-9457-7

Bures, O. (2017). Contributions of private businesses to the provision of security in the EU: beyond public-private partnerships. *An Interdisciplinary Journal, 67*(3), 289-312. doi:10.1007/s10611-016-9650-6

Bürgener, M., Snyman, N., & Hauck, M. (2001). *Towards a sustainable wildlife trade: an analysis of nature conservation legislation in South Africa with particular reference to the wildlife trade*. Retrieved from Institute of Criminology, University of Cape Town: South Africa: https://www.traffic.org/site/assets/files/10040/nature-conservation-legslation-in-south-africa-1.pdf. [February 7th 2020]

Button, M. (2019). *Private policing* (Second Edition. ed.). Abingdon, Oxon ; New York, NY: Routledge.

Button, M. (2020). The "New" Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions. *Journal of Contemporary Criminal Justice, 36*(1), 39-55. doi:10.1177/1043986219890194

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. London: Routledge.

Buxton, J., & Bingham, T. (2015). *The rise and challenge of Dark Net drug markets*. Retrieved from Global Drug Policy Observatory:

Cabral, L. (2012). The Oxford Handbook of the Digital Economy. In: Oxford University Press.

Cabral, L. M. B., & Hortacsu, A. (2004). *The Dynamics of Seller Reputation: Theory and Evidence from eBay*. Cambridge, Mass: National Bureau of Economic Research.

Campana, P., & Varese, F. (2013). Cooperation in criminal organizations: Kinship and violence as credible commitments. *Rationality and Society, 25*(3), 263-289. doi:10.1177/1043463113481202

Carrapico, H., & Farrand, B. (2017). 'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers.(Report)(Author abstract). *Crime, Law and Social Change, 67*(3), 245. doi:10.1007/s10611-016-9652-4

CESS Nuffield. (2019). Run experiments. Retrieved from https://cess-nuffield.nuff.ox.ac.uk/run-experiments/. [January 24th 2019]

Chainanalysis. (2021). *Crypto Crime Report*. Retrieved from https://blog.chainalysis.com/reports/darknet-markets-2021-geographic-breakdown. [February 24th 2021]

Challender, D. W., Wu, S. B., Nijman, V., & Macmillan, D. C. (2014). Changing behavior to tackle the wildlife trade. *Frontiers in Ecology and the Environment, 12*(4), 203-203. doi:10.1890/1540-9295-12.4.203

Chamberlin, E. H. (1948). An Experimental Imperfect Market. *Journal of Political Economy, 56*(2), 95-108. doi:10.1086/256654

Charrow, V. R., & Erhardt, M. K. (1986). *Clear and effective legal writing*. Boston: Little, Brown and Co.

Cherney, A., O'Reilly, J., & Grabosky, P. (2006). The Multilateralization of Policing: The Case of Illicit Synthetic Drug Control. *Police Practice and Research, 7*(3), 177-194. doi:10.1080/15614260600825398

Chiu, Y.-N., Leclerc, B., & Townsley, M. (2011). Crime Script Analysis of Drug Manufacturing In Clandestine Laboratories. *The British Journal of Criminology, 51*(2), 355-374. doi:10.1093/bjc/azr005

Cho, S. Y., & Wright, J. (2019). Into the Dark: A Case Study of Banned Darknet Drug Forums. In I. Weber, et al. (Ed.), *International Conference on Social Informatics. SocInfo 2019* (Vol. 11864, pp. 109-127): Cham: Springer International Publishing.

Christin, N. (2013). Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace. In (pp. 213-224). Proceedings of the 22nd international conference on world wide web.

CITES. (2020a). How CITES works. Retrieved from https://cites.org/eng/disc/how.php. [January 4th 2020]

CITES. (2020b). What is CITES. Retrieved from https://cites.org/eng/disc/what.php. [January 4th 2020]

Coalition to End Wildlife Trafficking Online. (2020). *Offline and in the wild: a progress report of the Coalition to End Wildlife Trafficking Online*. Retrieved from https://www.traffic.org/site/assets/files/12661/offline-and-in-the-wild.pdf. [March 4th 2020]

Sweet (Director). (2020). Cocaine, Synthetics, Heroin, Meth, Cannabis, Opioids [Television series episode]. In Collins, C., & et al (Executive producer), *The Business of Drugs*: Netflix.

Conradt, C. (2012). Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case. *International Journal of Cyber Criminology, 6*(1), 912-923.

Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), (1973).

Cordner, G. (2010). Reducing Fear of Crime: Strategies for Police. *Washington, DC: Office of Community Oriented Policing Services.* Retrieved from https://cops.usdoj.gov/RIC/Publications/cops-p173-pub.pdf. [June 27th 2021]

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies, 3*, 151-196.

Courchamp, F., Angulo, E., Rivalan, P., Hall, R. J., Signoret, L., Bull, L., & Meinard, Y. (2006). Rarity Value and Species Extinction: The Anthropogenic Allee Effect (The Anthropogenic Allee Effect). *PLoS Biology, 4*(12), e415. doi:10.1371/journal.pbio.0040415

Crawford, A. (2003). The pattern of policing in the UK: policing beyond the police. In T. Newburn (Ed.), *The handbook of policing* (pp. 136-168). Cullompton: Willan.

Crawford, A. (2011). Plural policing in the UK: policing beyond the police. In T. Newburn (Ed.), *Handbook of Policing*. London: Routledge.

Critchley, T. A. (1978). *A history of police in England and Wales* (Revised ed.). London: Constable.

CSIP. (2012). Mastercard Works With Interpol to Keep Consumers Safe. Retrieved from https://safemedsonline.org/2012/11/mastercard-works-interpol-keep-consumers-safe/. [February 1st 2021]

CSIP. (2013a). Black Market Site "Silk Road" Re-emerges. Retrieved from https://safemedsonline.org/2013/11/black-market-site-silk-road-re-emerges/. [February 1st 2021]

CSIP. (2013b). Companies Join Forces to Protect Consumers from the Prevalent Threat of Illegal Online Pharmacies. Retrieved from https://safemedsonline.org/2013/05/companies-join-forces-to-protect-consumers-from-the-prevalent-threat-of-illegal-online-pharmacies/. [February 1st 2021]

CSIP. (2013c). Google Taking Steps to Curtail Counterfeit Pharmacies. Retrieved from https://safemedsonline.org/2013/07/google-taking-steps-to-curtail-counterfeit-pharmacies/. [February 1st 2021]

CSIP. (2013d). Major Underground Online Drug Market Shut Down. Retrieved from https://safemedsonline.org/2013/10/major-underground-online-drug-market-shut-down/. [February 1st 2021]

CSIP. (2014a). CSIP Member Microsoft Opens Center to Fight Cybercrime. Retrieved from https://safemedsonline.org/2014/03/csip-member-microsoft-opens-center-fight-cybercrime/. [February 1st 2021]

CSIP. (2014b). CSIP Participates in Global Law Enforcement Operation Targeting Fake Medicines. Retrieved from https://safemedsonline.org/2014/05/csip-participates-in-global-law-enforcement-operation-targeting-fake-medicines/. [February 1st 2021]

CSIP. (2014c). CSIP Partners Help Shut Down Rogue Online Pharmacies. Retrieved from https://safemedsonline.org/2014/02/csip-partners-help-shut-rogue-online-pharmacies/. [February 21st 2021]

CSIP. (2014d). Operation Pangea VII Targets Social Media. Retrieved from https://safemedsonline.org/2014/06/operation-pangea-vii-targets-social-media/. [February 1st 2021]

CSIP. (2014e). Rogue Online Drug Marketplaces Pose Dangers for Consumers. Retrieved from https://safemedsonline.org/2014/07/rogue-online-drug-marketplaces-pose-dangers-consumers/. [February 1st 2021]

CSIP. (2016a). Operation Pangea VIII Targets Illicit Websites and Medical Devices. Retrieved from https://safemedsonline.org/2016/01/operation-pangea-viii-targets-illicit-websites-and-medical-devices/. [February 1st 2021]

CSIP. (2016b). Our Members: Continuing the Fight Against Rogue Online Pharmacies. Retrieved from https://safemedsonline.org/2016/09/our-members-continuing-the-fight-against-rogue-online-pharmacies/. [February 1st 2021]

CSIP. (2016c). Our Members: Fighting Against Rogue Online Pharmacies. Retrieved from https://safemedsonline.org/2016/07/members-fighting-rogue-online-pharmacies/. [February 1st 2021]

CSIP. (2017). Operation Pangea X Successfully Targets Websites Selling Fake Opioids and other Dangerous Drugs. Retrieved from https://safemedsonline.org/2017/10/operation-pangea-x-successfully-targets-websites-selling-fake-opioids-dangerous-drugs/. [February 1st 2021]

CSIP. (2018). Facebook Changes Ad Policies for Addiction Treatment Centers to Protect Consumers. Retrieved from https://safemedsonline.org/2018/09/facebook-changes-ad-policies-addiction-treatment-centers-protect-consumers/. [February 1st 2021]

CSIP. (2020a). CSIP Urges Consumers to Report Fraudulent Medications that Claim to Treat or Prevent COVID-19. Retrieved from https://safemedsonline.org/2020/03/csip-urges-consumers-to-report-fraudulent-medications-that-claim-to-treat-or-prevent-covid-19/. [February 1st 2021]

CSIP. (2020b). Tracking Illegal Opioid Sales Using Social Media Data. Retrieved from https://safemedsonline.org/2020/02/tracking-illegal-opioid-sales-using-social-media-data/. [February 1st 2021]

CSIP. (2021a). Who we are. Retrieved from https://safemedsonline.org/who-we-are/. [February 1st 2021]

CSIP. (2021b). Who we are - Missions, goals & objectives. Retrieved from https://safemedsonline.org/who-we-are/mission-goals-objectives/. [February 1st 2021]

Cugniere, L., Wright, J., & Milner-Gulland, E. J. (2019). Evidence to action: research to address illegal wildlife trade. *53*(3), 411-411. doi:10.1017/S0030605319000371

Cyjax. (2017). The Darknet after AlphaBay and Hansa. Retrieved from https://www.cyjax.com/2017/08/31/the-darknet-after-alphabay-and-hansa/. [April 21st 2020]

Cyjax. (2018a). Darknet markets: no honour among thieves. Retrieved from https://www.cyjax.com/2018/01/04/darknet-markets-no-honour-among-thieves/. [April 21st 2020]

Cyjax. (2018b). Darknet Review - April. Retrieved from https://www.cyjax.com/2018/04/24/darknet-review-24-april-2018/. [April 21st 2020]

Cyjax. (2018c). Hiding in plain sight - child abusers on the Darknet. Retrieved from https://www.cyjax.com/2018/01/15/hiding-in-plain-sight-child-abusers-on-the-darknet/. [April 21st 2020]

Cyjax. (2020a). About us. Retrieved from https://www.cyjax.com/company/. [April 21st 2020]

Cyjax. (2020b). Cyber threat services. Retrieved from https://www.cyjax.com/cyber-threat-services/. [April 21st 2020]

Cyjax. (2020c). Darknet Quartely Review - Q2 2020. Retrieved from https://www.cyjax.com/2020/07/09/darknet-quarterly-review-q2-2020/. [October 21st 2020]

Cyjax. (2020d). Darknet Quarterly Review. Retrieved from https://www.cyjax.com/2020/03/20/cyjax-darknet-quarterly-review/. [April 21st 2020]

Cyjax. (2020e). Incident response. Retrieved from https://www.cyjax.com/incident-response/. [April 21st 2020]

Cyjax. (2020f). Insights. Retrieved from https://www.cyjax.com/insights/. [April 21st 2020]

Dasgupta, P. (1990). Trust as a commodity. In D. Gambetta (Ed.), *Trust - Making and breaking cooperative relations* (pp. 49 - 72). Cambridge, Massachusetts: Basil Blackwell.

Davis, D. D., & Holt, C. A. (1993). *Experimental economics*. Princeton: Princeton University Press.

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime, 14*(2-3), 175-196. doi:10.1080/17440572.2013.801015

Décary-Hétu, D., & Giommoni, L. (2016). 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

Decary-Hetu, D., & Laferriere, D. (2015). Discreting vendors in online criminal markets. In G. Bichler & A. E. Malm (Eds.), *Disrupting criminal networks: network analysis in crime prevention*: Boulder: Lynne Rienner.

Dehghanniri, H., & Borrion, H. (2019). Crime scripting: A systematic review. *European Journal of Criminology*, 147737081985094. doi:10.1177/1477370819850943

Dellarocas, C. (2003). The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms. *Management Science, 49*(10), 1407-1424. doi:10.1287/mnsc.49.10.1407.17308

Dellarocas, C., & Wood, C. A. (2008). The Sound of Silence in Online Feedback: Estimating Trading Risks in the Presence of Reporting Bias. *Management Science, 54*(3), 460-476. doi:10.1287/mnsc.1070.0747

Dellarocas, C. N. (2001). Building Trust On-Line: The Design of Reliable Reputation Reporting : Mechanisms for Online Trading Communities. *SSRN Electronic Journal*. doi:10.2139/ssrn.289967

Delpeuch, T., & Ross, J. E. (2016). *Comparing the democratic governance of police intelligence : new models of participation and expertise in the United States and Europe*. Cheltenham, UK ; Northampton, MA, USA: EE, Edward Elgar Publishing.

Dittus, M., Wright, J., & Graham, M. (2018). Platform criminalism: the last-mile geography of the darknet market supply chain. In: Association for Computing Machinery.

Dixit, A. K. (2004). *Lawlessness and economics : alternative modes of governance*. Princeton ; Oxford: Princeton University Press.

Dolliver, D. S., Ericson, S. P., & Love, K., L. (2018). A geographic analysis of drug trafficking patterns on the tor network. *Geographical Review, 108*(1), 45-68.

Du, N., Huang, H., & Li, L. (2013). Can online trading survive bad-mouthing? An experimental investigation. *Decision Support Systems, 56*(1), 419-426. doi:10.1016/j.dss.2012.10.054

Duijn, P. A., Kashirin, V., & Sloot, P. M. (2014). The relative ineffectiveness of criminal network disruption. *Sci Rep, 4*, 4238. doi:10.1038/srep04238

Dupont, B. (2004). Security in the age of networks. *Policing & society, 14*(1), 76-91. doi:10.1080/1043946042000181575

Dupont, B. (2016a). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change, 67*(1), 97-116. doi:10.1007/s10611-016-9649-z

Dupont, B. (2016b). La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale. *Cultures & Conflits, n 102*(2), 95-120.

Dupont, B. (2016c). Les liens faibles du crime en ligne. *Réseaux, n 197-198*(3), 109-136. doi:10.3917/res.197.0109

Dupont, B., Côté, A.-M., Boutin, J.-I., & Fernandez, J. (2017). Darkode: Recruitment Patterns and Transactional Features of "the Most Dangerous Cybercrime Forum in the World". *American Behavioral Scientist, 61*(11), 1219-1243. doi:10.1177/0002764217734263

Dupont, B., Côté, A.-M., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime, 17*(2), 129-151. doi:10.1080/17440572.2016.1157480

eBay. (2008a). eBay To Institute Global Ban on Ivory Sales. Retrieved from https://www.ebayinc.com/stories/news/ebay-to-institute-global-ban-on-ivory-sales/. [March 27th 2020]

eBay. (2008b). IFAW Applauds eBay for Global Ivory Ban; An Interview with Barbara Cartwright, IFAW Campaign Manager. Retrieved from https://www.ebayinc.com/stories/news/ifaw-applauds-ebay-for-global-ivory-ban-an-interview-with-barbara-cartwright-ifaw-campaign-manager/. [March 27th 2020]

eBay. (2016a). *Global Impact 2016 report*. Retrieved from https://static.ebayinc.com/assets/Uploads/Documents/eBay-Global-Impact-2016Summary.pdf. [March 27th 2020]

eBay. (2016b). On Earth Day and Every Day, eBay is Working to End Wildlife Trafficking. Retrieved from https://www.ebayinc.com/stories/news/on-earth-day-and-every-day/. [March 27th 2020]

eBay. (2016c). Working Together to End Wildlife Trafficking. Retrieved from https://www.ebayinc.com/stories/news/working-together-to-end-wildlife-trafficking/. [March 27th 2020]

eBay. (2017a). *eBay Impact 2017 Progress Update*. Retrieved from https://static.ebayinc.com/assets/Uploads/Documents/eBay-Impact-2017-Progress-Update.pdf. [March 27th 2020]

eBay. (2017b). Taking Steps to Combat Illegal Wildlife Trafficking. Retrieved from https://www.ebayinc.com/stories/news/taking-steps-to-combat-illegal-wildlife-trafficking/. [March 27th 2020]

eBay. (2018a). *eBay Impact 2018 Progress Update*. Retrieved from https://static.ebayinc.com/assets/Uploads/Documents/eBay-Impact-2018-Progress-Update.pdf. [March 27th 2020]

eBay. (2018b). Supporting World Elephant Day. Retrieved from HTTPS://WWW.EBAYINC.COM/STORIES/NEWS/SUPPORTING-WORLD-ELEPHANT-DAY/. [March 27th 2020]

eBay. (2019a). eBay Celebrates Global Tiger Day with World Wildlife Fund. Retrieved from HTTPS://WWW.EBAYINC.COM/STORIES/NEWS/EBAY-CELEBRATES-GLOBAL-TIGER-DAY-WITH-WORLD-WILDLIFE-FUND/. [March 27th 2020]

eBay. (2019b). eBay Partners With the International Fund for Animal Welfare in Honor of its 10-Year Anniversary on the Global Ban of Ivory Sales. Retrieved from HTTPS://WWW.EBAYINC.COM/STORIES/NEWS/EBAY-PARTNERS-WITH-THE-INTERNATIONAL-FUND-FOR-ANIMAL-WELFARE-IN-HONOR-OF-ITS-10-YEAR-ANNIVERSARY-ON-THE-GLOBAL-BAN-OF-IVORY-SALES/. [March 27th 2020]

eBay. (2020a). Animal products policy. Retrieved from https://www.ebay.co.uk/help/policies/prohibited-restricted-items/animal-products-policy?id=5046. [March 27th 2020]

eBay. (2020b). Illegal drugs and drug paraphernalia policy. Retrieved from https://www.ebay.com/help/policies/prohibited-restricted-items/illegal-drugs-drug-paraphernalia-policy?id=4333&st=12&pos=1&query=Illegal%20drugs%20and%20drug%20paraphernalia%20policy&intent=drug. [April 4th 2020]

eBay. (2020c). Live animals policy. Retrieved from https://www.ebay.com/help/policies/prohibited-restricted-items/zoo-animals-wildlife-products-policy?id=4327. [March 27th 2020]

eBay. (2020d). Prescription and over-the-counter drugs policy. Retrieved from https://www.ebay.com/help/policies/prohibited-restricted-items/prescription-overthecounter-drugs-policy?id=5048&st=12&pos=2&query=Prescription%20and%20over-the-counter%20drugs%20policy&intent=drug. [April 4th 2020]

eBay. (2020e). Report an item or listing. Retrieved from https://www.ebay.com/help/policies/member-behavior-policies/report-item-listing?id=4739&st=2&pos=2&query=Report%20an%20item%20or%20listing&intent=report. [March 27th 2020]

EMCDDA. (2020). *EMCDDA Special Report. COVID-19 and drugs - Drug supply via darknet markets*. Retrieved from https://www.emcdda.europa.eu/system/files/publications/13042/EMCDDA-report_COVID19-darknet-final.pdf. [February 24th 2021]

EMCDDA. (2021). About the EMCDDA. Retrieved from https://www.emcdda.europa.eu/about. [April 24th 2021]

EMCDDA, & Europol. (2005). *Annual Report on the implementation of Council Decision 2005/387/JHA*. Retrieved from http://www.emcdda.europa.eu/html.cfm/index132877EN.html. [March 17th 2020]

EMCDDA, & Europol. (2007). *Joint Report on a new psychoactive substance: 1-benzylpiperazine (BZP)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-reports/bzp_en. [March 17th 2020]

EMCDDA, & Europol. (2008). *Annual Report on the implementation of Council Decision 2005/387/JHA*. Retrieved from http://www.emcdda.europa.eu/html.cfm/index132901EN.html_ru. [March 17th 2020]

EMCDDA, & Europol. (2009). *Annual Report on the implementation of Council Decision 2005/387/JHA*. Retrieved from http://www.emcdda.europa.eu/html.cfm/index132910EN.html_ru. [March 17th 2020]

EMCDDA, & Europol. (2010a). *Annual Report on the implementation of Council Decision 2005/387/JHA*. Retrieved from http://www.emcdda.europa.eu/publications/implementation-reports/2010_ru. [March 17th 2020]

EMCDDA, & Europol. (2010b). *Joint Report on a new psychoactive substance: 4-methylmethcathinone (mephedrone)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-reports/mephedrone_en. [March 17th 2020]

EMCDDA, & Europol. (2011). *Annual Report on the implementation of Council Decision 2005/387/JHA*. Retrieved from http://www.emcdda.europa.eu/publications/implementation-reports/2011_ru. [March 17th 2020]

EMCDDA, & Europol. (2012a). *Joint Report on a new psychoactive substance: 4-methylamphetamine*. Retrieved from http://www.emcdda.europa.eu/publications/joint-reports/4-ma_en. [March 17th 2020]

EMCDDA, & Europol. (2012b). *New drugs in Europe - Annual Report on the implementation of Council Decision 2005/387/JHA*. Retrieved from http://www.emcdda.europa.eu/publications/implementation-reports/2012_en. [March 17th 2020]

EMCDDA, & Europol. (2013a). *Annual Report on the implementation of Council Decision 2005/387/JHA*. Retrieved from http://www.emcdda.europa.eu/publications/implementation-reports/2013_ru. [March 17th 2020]

EMCDDA, & Europol. (2013b). *EU drug markets report - a strategic analysis*. Retrieved from http://www.emcdda.europa.eu/publications/joint-publications/drug-markets_en. [March 17th 2020]

EMCDDA, & Europol. (2013c). *Joint Report on a new psychoactive substance: 5-(2-aminopropyl)indole (5-IT)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-reports/5-IT_en. [March 17th 2020]

EMCDDA, & Europol. (2014a). *Annual Report on the implementation of Council Decision 2005/387/JHA*. Retrieved from http://www.emcdda.europa.eu/publications/implementation-reports/2014_ru. [March 17th 2020]

EMCDDA, & Europol. (2014b). *Joint Report on a new psychoactive substance: 1-cyclohexyl-4- (1,2-diphenylethyl)piperazine ('MT-45')*. Retrieved from http://www.emcdda.europa.eu/publications/joint-reports/MT-45_en. [March 17th 2020]

EMCDDA, & Europol. (2014c). *Joint Report on a new psychoactive substance: 4,4'-DMAR (4-methyl-5- (4-methylphenyl)-4,5-dihydrooxazol-2-amine)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-reports/4-4-DMAR_en. [March 17th 2020]

EMCDDA, & Europol. (2014d). *Joint Report on a new psychoactive substance: 25I-NBOMe (4-iodo-2,5- dimethoxy-N-(2-methoxybenzyl)phenethylamine)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-report/25I-NBOMe_en. [March 17th 2020]

EMCDDA, & Europol. (2014e). *Joint Report on a new psychoactive substance: AH-7921 3,4-dichloro-N-{[1-(dimethylamino)cyclohexyl] methyl}benzamide*. Retrieved from http://www.emcdda.europa.eu/publications/risk-assessment/AH-7921_en. [March 17th 2020]

EMCDDA, & Europol. (2014f). *Joint Report on a new psychoactive substance: MDPV (3,4-methylenedioxypyrovalerone)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-report/MDPV_en. [March 17th 2020]

EMCDDA, & Europol. (2014g). *Joint Report on a new psychoactive substance: methoxetamine (2-(3-methoxyphenyl)-2-(ethylamino) cyclohexanone)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-report/methoxetamine_en. [March 17th 2020]

EMCDDA, & Europol. (2015). *Annual Report on the implementation of Council Decision 2005/387/JHA*. Retrieved from http://www.emcdda.europa.eu/publications/implementation-reports/2015_ru. [March 17th 2020]

EMCDDA, & Europol. (2016a). *Annual Report on the implementation of Council Decision 2005/387/JHA*. Retrieved from http://www.emcdda.europa.eu/publications/implementation-reports/2016_ru. [March 17th 2020]

EMCDDA, & Europol. (2016b). *EU drug market markets report - in-depth analysis*. Retrieved from http://www.emcdda.europa.eu/publications/joint-publications/eu-drug-markets-2016-in-depth-analysis_en. [March 17th 2020]

EMCDDA, & Europol. (2016c). *Joint Report on a new psychoactive substance: methyl 2-[[1-(cyclohexylmethyl)indole-3-carbonyl]amino]- 3,3-dimethylbutanoate (MDMB-CHMICA)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-reports/mdmb-chmica_en. [March 17th 2020]

EMCDDA, & Europol. (2016d). *Joint Report on a new psychoactive substance: N-phenyl-N-[1-(2-phenylethyl)piperidin-4-yl] acetamide (acetylfentanyl)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-reports/acetylfentanyl_en. [March 17th 2020]

EMCDDA, & Europol. (2017a). *Drugs and the darknet - perspectives for enforcement, research and policy*. Retrieved from http://www.emcdda.europa.eu/publications/joint-publications/drugs-and-the-darknet_en. [March 17th 2020]

EMCDDA, & Europol. (2017b). *Joint Report on a new psychoactive substance: N-(1-phenethylpiperidin-4-yl)- N-phenylacrylamide (acryloylfentanyl)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-reports/acryloylfentanyl_en. [March 17th 2020]

EMCDDA, & Europol. (2017c). *Joint Report on a new psychoactive substance: N-phenyl-N-[1-(2-phenylethyl) piperidin-4-yl]-furan-2-carboxamide (furanylfentanyl)*. Retrieved from http://www.emcdda.europa.eu/publications/joint-reports/furanylfentanyl_en. [March 17th 2020]

EMCDDA, & Europol. (2019). *EU drug markets report*. Retrieved from http://www.emcdda.europa.eu/publications/joint-publications/eu-drug-markets-report-2019_en. [March 17th 2020]

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine, 7*(3), 93-99.

Espinosa, R. (2019). Scamming and the reputation of drug dealers on Darknet Markets. *International Journal of Industrial Organization, 67*. doi:10.1016/j.ijindorg.2019.102523

Etsy. (2016). Company News - Working Together to End Illegal Wildlife Trafficking. Retrieved from https://blog.etsy.com/news/2016/working-together-to-end-illegal-wildlife-trafficking/. [March 30th 2020]

Etsy. (2020). Prohibited Items Policy. Retrieved from https://www.etsy.com/uk/legal/prohibited/?ref=list. [March 30th 2020]

Eurojust, & Europol. (2019). *Common challenges in combatting cybercrime*. Retrieved from http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20(June%202019)/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF. [March 17th 2020]

European Union Wildlife and Trade regulation, (1996).

Europol. (2004). *European Union Organised Crime Report*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european-union-organised-crime-report-2004. [March 17th 2020]

Europol. (2005). *European Union Organised Crime Report*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european-union-organised-crime-report-2005. [March 17th 2020]

Europol. (2006). *European Union Organised Crime Threat Assessment (OCTA)*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/octa-2006-eu-organised-crime-threat-assessment. [March 17th 2020]

Europol. (2008). *European Union Organised Crime Threat Assessment (OCTA)*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/octa-2008-eu-organised-crime-threat-assessment. [March 17th 2020]

Europol. (2011a). *European Union Organised Crime Threat Assessment (OCTA)*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/octa-2011-eu-organised-crime-threat-assessment. [March 17th 2020]

Europol. (2011b). *OC-SCAN policy brief - trafficking in endangered species by organised crime groups*. Retrieved from https://www.europol.europa.eu/publications-documents/oc-scan-threat-notice-trafficking-of-endangered-species. [March 17th 2020]

Europol. (2012). *Europol Review - general report on Europol activities*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/europol-review-2012. [March 17th 2020]

Europol. (2013a). *European Union Serious and Organised Crime Threat Assessment (SOCTA)*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/eu-serious-and-organised-crime-threat-assessment-socta-2013. [March 17th 2020]

Europol. (2013b). *Threat assessment 2013 environmental crime in the EU*. Retrieved from https://www.europol.europa.eu/publications-documents/threat-assessment-2013-environmental-crime-in-eu. [March 17th 2020]

Europol. (2014a). *EC3 first year report*. Retrieved from https://www.europol.europa.eu/publications-documents/european-cybercrime-center-ec3-first-year-report. [March 17th 2020]

Europol. (2014b). *Europol Review - general report on Europol activities*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/europol-review-2014. [March 17th 2020]

Europol. (2014c). *Global action against Dark Markets on Tor network*. Retrieved from https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network?ncid=txtlnkusaolp00000618. [March 17th 2020]

Europol. (2014d). *Internet Organised Crime Threat Assessment (IOCTA)*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014. [March 17th 2020]

Europol. (2015a). *EnviCrimeNet Intelligence Project on Environmental Crime - report on environmental crime in Europe*. Retrieved from https://www.europol.europa.eu/publications-documents/report-environmental-crime-in-europe. [March 17th 2020]

Europol. (2015b). *Europol Review - general report on Europol activities*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/europol-review-2015. [March 17th 2020]

Europol. (2015c). *Internet Organised Crime Threat Assessment (IOCTA)*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015. [March 17th 2020]

Europol. (2016a). *Europol and EMCDDA: excellent cooperation to combat the illicit drug markets in the EU*. Retrieved from https://www.europol.europa.eu/newsroom/news/europol-and-emcdda-excellent-cooperation-to-combat-illicit-drug-markets-in-eu-0. [March 17th 2020]

Europol. (2016b). *Internet Organised Crime Threat Assessment (IOCTA)*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016. [March 17th 2020]

Europol. (2017a). Darknet dealer of drugs and arms arrested by Slovak authorities. Retrieved from https://www.europol.europa.eu/newsroom/news/darknet-dealer-of-drugs-and-arms-arrested-slovak-authorities. [March 17th 2020]

Europol. (2017b). *Drugs and the darknet - perspectives for enforcement, research and policy*. Retrieved from https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy. [March 17th 2020]

Europol. (2017c). *Drugs in Europe: a bold Law Enforcement response*. Retrieved from https://www.europol.europa.eu/newsroom/news/drugs-in-europe-bold-law-enforcement-response. [March 17th 2020]

Europol. (2017d). *Europol Review 2016-2017*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/europol-review-2016-2017. [March 17th 2020]

Europol. (2017e). *Internet Organised Crime Threat Assessment (IOCTA)*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017. [March 17th 2020]

Europol. (2017f). Massive blow to criminal dark web activities after globally coordinated operation. Retrieved from https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation. [July 14th 2019]

Europol. (2017g). *Serious and Organised Crime Threat Assessment (SOCTA)*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017. [March 1st 2019]

Europol. (2018a). *Crime on the dark web: law enforcement coordination is the only cure*. Retrieved from https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure. [March 17th 2020]

Europol. (2018b). *'Drugs in Europe: a bold law enforcement response' second annual conference*. Retrieved from https://www.europol.europa.eu/newsroom/news/%E2%80%98drugs-in-europe-bold-law-enforcement-response%E2%80%99-second-annual-conference. [March 17th 2020]

Europol. (2018c). *Internet Organised Crime Threat Assessment (IOCTA)*. Retrieved from https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. [March 17th 2020]

Europol. (2019a). Deepdotweb shut down: administrators suspected of receiving millions of kickbacks from illegal dark web proceeds. Retrieved from https://www.europol.europa.eu/newsroom/news/deepdotweb-shut-down-administrators-suspected-of-receiving-millions-of-kickbacks-illegal-dark-web-proceeds. [July 14th 2019]

Europol. (2019b). Double blow to dark web marketplaces. Retrieved from https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces. [July 14th 2019]

Europol. (2019c). Europol's 20 most noteworthy operations. Retrieved from https://www.europol.europa.eu/about-europol/europols-20-most-noteworthy-operations. [July 14th 2019]

Europol. (2019d). Global Law Enforcement action against vendors and buyers on the Dark Web. Retrieved from https://www.europol.europa.eu/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web. [July 14th 2019]

Europol. (2019e). *Illicit drugs in the EU: the situation is expanding in scale and complexity*. Retrieved from https://www.europol.europa.eu/newsroom/news/illicit-drugs-in-eu-situation-expanding-in-scale-and-complexity. [March 17th 2020]

Europol. (2019f). International drug trafficking network disrupted. Retrieved from https://www.europol.europa.eu/newsroom/news/international-drug-trafficking-network-disrupted. [March 17th 2020]

Europol. (2019g). Internet Organised Crime Threat Assessment (IOCTA). Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019. [October 9th 2019]

Europol. (2019h). xDedic marketplace shut down in international operation. Retrieved from https://www.europol.europa.eu/newsroom/news/xdedic-marketplace-shut-down-in-international-operation. [July 14th 2019]

Europol. (2020a). 28 bird traffickers netting €1 million per year arrested in Spain. Retrieved from https://www.europol.europa.eu/newsroom/news/28-bird-traffickers-netting-€1-million-year-arrested-in-spain. [October 21st 2020]

Europol. (2020b). About Europol. Retrieved from https://www.europol.europa.eu/about-europol. [September 1st 2020]

Europol. (2020c). Europol History. Retrieved from https://www.europol.europa.eu/history/europol-history.html. [September 1st 2020]

Europol. (2020d). International sting against Dark Web vendors leads to 179 arrests. Retrieved from https://www.europol.europa.eu/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests. [October 21st 2020]

Europol. (2020e). Internet Organised Crime Threat Assessment (IOCTA). Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020. [October 21st 2020]

Europol. (2020f). Polish police take criminal gang selling fake impotence treatments off the market. Retrieved from https://www.europol.europa.eu/newsroom/news/polish-police-take-criminal-gang-selling-fake-impotence-treatments-market. [October 21st 2020]

Europol. (2020g). Spain and Portugal take illegal ivory off the black market. Retrieved from https://www.europol.europa.eu/newsroom/news/spain-and-portugal-take-illegal-ivory-black-market. [March 17th 2020]

Europol. (2021a). 800 criminals arrested in biggest ever law enforcement operation against encrypted communication. Retrieved from https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication. [June 17th 2021]

Europol. (2021b). *The cyber blue line*. Retrieved from Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.: https://www.europol.europa.eu/europol-spotlight/cyber-blue-line. [June 27th 2021]

Europol. (2021c). Darkmarket: world's largest illegal Dark Web marketplace taken down. Retrieved from https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down. [June 17th 2021]

Europol. (2021d). EC3 Partners. Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners. [July 7th 2021]

Europol. (2021e). *European Union Serious and Organised Crime Threat Assessment. A corrupting influence: the infiltration and undermining or Europe's economy and society by organised crime.* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment. [June 17th 2021]

Facebook. (2014). Facebook, Instagram Announce New Educational and Enforcement Measures for Commercial Activity. Retrieved from https://about.fb.com/news/2014/03/facebook-instagram-announce-new-educational-and-enforcement-measures-for-commercial-activity/. [April 2nd 2020]

Facebook. (2018a). How We Enforce Against Illicit Drug Sales. Retrieved from https://about.fb.com/news/2018/09/enforcing-against-drug-sales/. [April 2nd 2020]

Facebook. (2018b). Supporting Our Community in the Face of the Opioid Epidemic. Retrieved from https://about.fb.com/news/2018/11/force-for-good/. [April 2nd 2020]

Facebook. (2019a). Community Standards Enforcement Report, November 2019 Edition. Retrieved from https://about.fb.com/news/2019/11/community-standards-enforcement-report-nov-2019/. [April 2nd 2020]

Facebook. (2019b). An Update on How We Are Doing At Enforcing Our Community Standards. Retrieved from https://about.fb.com/news/2019/05/enforcing-our-community-standards-3/. [April 2nd 2020]

Facebook. (2020). Community standards - Regulated goods. Retrieved from https://www.facebook.com/communitystandards/regulated_goods/. [April 2nd 2020]

FDA. (2021). What we do. Retrieved from https://www.fda.gov/about-fda/what-we-do. [February 24th 2021]

Fennema, M., & Tillie, J. (1999). Political participation and political trust in Amsterdam: Civic communities and ethnic networks. *Journal of ethnic and migration studies, 25*(4), 703-726. doi:10.1080/1369183X.1999.9976711

Field, A. P., & Hole, G. (2003). *How to design and report experiments*. London ; Thousand Oaks, Calif.: Sage publications Ltd.

Fielding, N. (1995). *Community policing*. Oxford: Clarendon Press.

Flanagan, R. (2008). *The Review of Policing - Final Report*. Retrieved from https://www.justiceinspectorates.gov.uk/hmicfrs/media/flanagan-review-of-policing-20080201.pdf. [June 7th 2020]

Flashpoint. (2016). *2015 Highlights & Trends in the Deep & Dark Web*. Retrieved from https://www.flashpoint-intel.com/home/assets/File/Flashpoint_IlluminatingTheDeep&DarkWeb.pdf. [May 1st 2020]

Flashpoint. (2017a). Fentanyl Sales in the Deep & Dark Web. Retrieved from https://www.flashpoint-intel.com/blog/fentanyl-sales-deep-dark-web/. [May 1st 2020]

Flashpoint. (2017b). U.S. DOJ Announces Takedowns of AlphaBay and Hansa Underground Markets. Retrieved from https://www.flashpoint-intel.com/blog/doj-takedowns-alphabay-hansa/. [May 1st 2020]

Flashpoint. (2018a). Inside the Underground Trade of Prescription Drugs. Retrieved from https://www.flashpoint-intel.com/blog/prescription-drug-trade-in-the-cybercriminal-underground/. [May 1st 2020]

Flashpoint. (2018b). Wait Continues for AlphaBay Successor. Retrieved from https://www.flashpoint-intel.com/blog/wait-continues-alphabay-successor/. [May 1st 2020]

Flashpoint. (2019a). Expansive Access to Illicit Activity on Chat Services Platforms Lowers Risk. Retrieved from https://www.flashpoint-intel.com/blog/expansive-access-to-illicit-activity-on-chat-services-platforms-lowers-risk/. [May 1st 2020]

Flashpoint. (2019b). Looking at Darknet Marketplaces Through A Brazilian Lens. Retrieved from https://www.flashpoint-intel.com/blog/looking-at-darknet-marketplaces-through-a-brazilian-lens/. [May 1st 2020]

Flashpoint. (2020). Popular Narcotics across Illicit Online Communities and Marketplaces. Retrieved from https://www.flashpoint-intel.com/blog/popular-narcotics-across-illicit-online-communities-and-marketplaces/. [October 21st 2020]

Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). *An inquiry into the nature and causes of the wealth of Internet miscreants*. Paper presented at the ACM Conference on Computer and Communications Security (CCS), VA.

Freeads. (2019a). Birds checklist. Retrieved from https://help.freeads.co.uk/support/solutions/articles/47000873701-birds-checklist. [March 31st 2020]

Freeads. (2019b). Exotic animals checklist. Retrieved from https://help.freeads.co.uk/support/solutions/articles/47000874056-exotic-animals-checklist. [March 31st 2020]

Freeads. (2019c). Why is my ad not live yet? Retrieved from https://help.freeads.co.uk/support/solutions/articles/47000872636-why-is-my-ad-not-live-yet-. [March 31st 2020]

Freeads. (2020a). How to report an Advert. Retrieved from https://help.freeads.co.uk/support/solutions/articles/47000873005-how-to-report-an-advert. [March 31st 2020]

Freeads. (2020b). Pet Advert Posting Rules. Retrieved from https://help.freeads.co.uk/support/solutions/articles/47001104975-pet-advert-posting-rules. [March 31st 2020]

Freeads. (2020c). Posting rules. Retrieved from https://help.freeads.co.uk/support/solutions/articles/47000872678-posting-rules. [March 31st 2020]

Friedman, D., & Sunder, S. (1994). *Experimental methods : a primer for economists*. Cambridge: Cambridge University Press.

Friedman, E. J., & Resnick, P. (2001). The Social Cost of Cheap Pseudonyms. *Journal of Economics & Management Strategy, 10*(2), 173-199. doi:10.1111/j.1430-9134.2001.00173.x

Friedrichs, J. (2008). *Fighting terrorism and drugs : Europe and international police cooperation*. London: Routledge.

Fudenberg, D., Rand, D. G., & Dreber, A. (2012). Slow to Anger and Fast to Forgive: Cooperation in an Uncertain World. *American Economic Review, 102*(2), 720-749. doi:10.1257/aer.102.2.720

Gallo, E., Riyanto, Y. E., Roy, N., & Teh, T.-H. (2019). Cooperation in an Uncertain and Dynamic World. *SSRN Electronic Journal*. doi:10.2139/ssrn.3511476

Gallo, E., & Yan, C. (2015). The effects of reputational and social knowledge on cooperation. *Proceedings of the National Academy of Sciences of the United States of America, 112*(12), 3647-3652.

George, B., & Button, M. (2000). *Private security*. Leicester: Perpetuity.

Gooch, G., & Williams, M. (2015). A Dictionary of Law Enforcement. In (2 ed.): Oxford University Press.

Good, E. (1989). *Mightier than the sword, powerful writing in the legal profession*. Charlottesville, Va: Blue Jeans Press.

Goodman, M. D. (1997). Why the police don't care about computer crime. *Harvard Journal of Law and Technology, 10*(3), 465-495.

Greenberg, D. H., & Shroder, M. (2004). *The digest of social experiments* (Third ed.). Washington, D.C.: Urban Institute Press.

Greenfield, S., & Veríssimo, D. G. (2018). To what extent is social marketing used in demand reduction campaigns for illegal wildlife products? Insights from elephant ivory and rhino horn. *Social Marketing Quarterly, 25*. doi:10.1177/1524500418813543

Greif, A. (1991). The Organization of Long-Distance Trade: Reputation and Coalitions in the Geniza Documents and Genoa During the Eleventh and Twelfth Centuries. *The Journal of Economic History, 51*(2), 459-462. doi:10.1017/S0022050700039097

Gumtree. (2020a). Animals We Do Not Allow. Retrieved from https://help.gumtree.com/s/policies?cat=Pets_Policies&article=Animals-We-Do-Not-Allow. [March 31st 2020]

Gumtree. (2020b). Pet Policies. Retrieved from https://help.gumtree.com/s/policies?cat=Pets_Policies&article=Pets-Policies. [March 31st 2020]

Gumtree. (2020c). Protecting Pets by Making Our Pets Category Harder to Use. Retrieved from https://help.gumtree.com/s/policies?cat=Pets_Policies&article=Protecting-Pets-by-Making-Our-Pets-Category-Harder-to-Use2. [March 31st 2020]

Gumtree. (2020d). Reporting an ad. Retrieved from https://help.gumtree.com/s/safety?cat=Reporting_Bad_Activity&article=Reporting-an-Ad. [March 31st 2020]

Gumtree. (2020e). What's not allowed on Gumtree. Retrieved from https://help.gumtree.com/s/policies?cat=Posting_Policies&article=What-s-Not-Allowed-on-Gumtree. [March 31st 2020]

Harrison, J. R., Roberts, D. L., & Hernandez-Castro, J. (2016). Assessing the extent and nature of wildlife trade on the dark web. *Conservation Biology, 30*(4), 900-904. doi:10.1111/cobi.12707

Heckman, J. J., & Smith, J. A. (1995). Assessing the Case for Social Experiments. *Journal of Economic Perspectives, 9*(2), 85-110. doi:10.1257/jep.9.2.85

Helmond, A. (2015). The Platformization of the Web: Making Web Data Platform Ready. *Social media + society, 1*(2). doi:10.1177/2056305115603080

Herbert, S. (1999). The end of the territorially-sovereign state? The case of crime control in the United States. *Political geography, 18*(2), 149-172. doi:10.1016/S0962-6298(98)00080-8

Herley, C., & Florencio, D. (2009). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. *Microsoft Research*.

Hobbes, T. (1651). *Leviathan*. Cambridge: Cambridge University Press.

Hoe, S., Kantarcioglu, M., & Bensoussan, A. (2012). A game theoretical analysis of lemonising cybercriminal black markets. In J. Grossklags & J. Walrand (Eds.), *Decision and game theory for security* (pp. 60-77). Third International Conference, GameSec 2012, Budapest, Hungary, November 5-6 Proceedings.

Holden, M. H., & McDonald-Madden, E. (2017). High prices for rare species can drive large populations extinct: the anthropogenic Allee effect revisited. *Journal of theoretical biology, 429*, 170-180. doi:10.1016/j.jtbi.2017.06.019

Holsti, O. R. (1969). *Content analysis for the social sciences and humanities*. Reading, Massachusetts ; London: Addison-Wesley.

Holt, C. A., & Sherman, R. (1999). Classroom Games: A Market for Lemons. *Journal of Economic Perspectives, 13*(1), 205-214. doi:10.1257/jep.13.1.205

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*. doi:10.1093/cybsec/tyw007

Hooghe, M., Stolle, D., Mahéo, V.-A., & Vissers, S. (2010). Why Can't a Student Be More Like an Average Person?: Sampling and Attrition Effects in Social Science Field and Laboratory Experiments. *The ANNALS of the American Academy of Political and Social Science, 628*(1), 85-96. doi:10.1177/0002716209351516

Houser, D., & Wooders, J. (2006). Reputation in Auctions: Theory, and Evidence from e Bay. *Journal of Economics & Management Strategy, 15*(2), 353-369. doi:10.1111/j.1530-9134.2006.00103.x

Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research, 15*(9), 1277-1288. doi:10.1177/1049732305276687

Hutchings, A., Clayton, R., & Anderson, R. (2016). Taking down websites to prevent crime. In (Vol. 2016-, pp. 1-10). IEEE.

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

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime, 18*(1), 11-30. doi:10.1080/17440572.2016.1197123

IFAW. (2004). *Elephants on the high street - An investigation into ivory trade in the UK*. Retrieved from https://s3.amazonaws.com/ifaw-pantheon/sites/default/files/legacy/Elephants%20on%20the%20high%20street%20an%20investigation%20into%20ivory%20trade%20in%20the%20UK%20-%202004.pdf. [March 4th 2020]

IFAW. (2005). *Caught in the web*. Retrieved from IFAW contact.

IFAW. (2007). *Bidding for extinction*. Retrieved from https://d1jyxxz9imt9yb.cloudfront.net/resource/75/attachment/regular/Report_2007_Bidding_for_Extinction.pdf. [March 4th 2020]

IFAW. (2008a). *Criminal nature - The Global Security Implications of the Illegal Wildlife Trade*. Retrieved from https://d1jyxxz9imt9yb.cloudfront.net/resource/151/attachment/original/Criminal_Nature_Global_security_and_wildlife_trade_2008.pdf. [March 4th 2020]

IFAW. (2008b). *Killing with Keystrokes: an investigation of the illegal wildlife trade on the World Wide Web*. Retrieved from https://s3.amazonaws.com/ifaw-pantheon/sites/default/files/legacy/Killing%20with%20Keystrokes.pdf. [March 4th 2020]

IFAW. (2011). *Killing with Keystrokes 2.0: IFAW's investigation into the European online ivory trade*. Retrieved from https://d1jyxxz9imt9yb.cloudfront.net/resource/203/attachment/original/FINAL_Killing_with_Keystrokes_2.0_report_2011.pdf. [March 4th 2020]

IFAW. (2012). *Making a killing - a 2011 survey of ivory markets in China*. Retrieved from https://s3.amazonaws.com/ifaw-pantheon/sites/default/files/legacy/Making%20a%20Killing.pdf. [March 4th 2020]

IFAW. (2013). *Criminal nature - the global security implications of the illegal wildlife trade*. Retrieved from https://d1jyxxz9imt9yb.cloudfront.net/resource/128/attachment/original/ifaw-criminal-nature-UK.pdf. [March 4th 2020]

IFAW. (2014a). *Bidding against survival - the elephant poaching crisis and the role of auctions in the US ivory market*. Retrieved from https://afbeeldingen.animalstoday.nl/IFAW-Ivory-Auctions-bidding-against-survival-aug-2014_0.pdf. [March 4th 2020]

IFAW. (2014b). *Click to delete - Australian websites selling endangered wildlife*. Retrieved from https://d1jyxxz9imt9yb.cloudfront.net/resource/127/attachment/original/IFAW_Internet_Trade_Report_AUS_final.pdf. [March 4th 2020]

IFAW. (2014c). *Elephant VS Mouse - an investigation of the ivory trade on Craigslist*. Retrieved from https://d1jyxxz9imt9yb.cloudfront.net/resource/154/attachment/regular/IFAW-craigslist-ivory-report-2015.pdf. [March 4th 2020]

IFAW. (2014d). *Wanted - Dead or Alive Exposing Online Wildlife Trade*. Retrieved from https://d1jyxxz9imt9yb.cloudfront.net/resource/251/attachment/original/IFAW-Wanted-Dead-or-Alive-Exposing-Online-Wildlife-Trade-2014.pdf. [March 4th 2020]

IFAW. (2017a). *Ivory Seizures in Europe 2006- 2015*. Retrieved from https://d1jyxxz9imt9yb.cloudfront.net/resource/275/attachment/original/ifaw-ivory-seizures-europe.pdf. [March 4th 2020]

IFAW. (2017b). *Out of Africa: byting down on wildlife cybercrime*. Retrieved from https://s3.amazonaws.com/ifaw-pantheon/sites/default/files/legacy/%28Pixelated%20Webversion%29SAInvestigationReport_lores.pdf. [March 4th 2020]

IFAW. (2018a). *Disrupt: Wildlide cybercrime. Uncovering the scale of online wildlife trade*. Retrieved from https://d1jyxxz9imt9yb.cloudfront.net/resource/1/attachment/regular/IFAW_-_Disrupt_Wildlife_Cybercrime_-_English.pdf. [March 4th 2020]

IFAW. (2018b). *Global wildlife cybercrime action plan - a call to action for the London Conference on Illegal Wildlife Trade*. Retrieved from

https://d1jyxxz9imt9yb.cloudfront.net/resource/31/attachment/original/Global_Wildlife_Cybercrime_Action_Plan.pdf. [March 4th 2020]

IFAW. (2020a). Our history. Retrieved from https://www.ifaw.org/uk/about/history. [March 4th 2020]

IFAW. (2020b). Programmes. Retrieved from https://www.ifaw.org/uk/about/programmes. [March 4th 2020]

Instagram. (2017). Protecting Wildlife and Nature From Exploitation. Retrieved from https://about.instagram.com/blog/announcements/protecting-against-harmful-wildlife-and-nature-content/. [March 31st 2020]

Instagram. (2020). Community guidelines. Retrieved from https://help.instagram.com/477434105621119. [March 31st 2020]

International Compliance Association. (2020). Solutions. *Wildlife Crime is Financial Crime: A collaborative approach in the fight against wildlife crime*. Online: October 16th.

Interpol. (2020). Pharmaceutical crime operations. Retrieved from https://www.interpol.int/en/Crimes/Illicit-goods/Pharmaceutical-crime-operations. [December 19th 2020]

Interpol, & IFAW. (2013). *Project Web - an investigation into the ivory trade over the Internet within the European Union*. Retrieved from https://d1jyxxz9imt9yb.cloudfront.net/resource/715/attachment/original/Project_Web.pdf. [March 4th 2020]

Jewkes, Y., & Yar, M. (2011). Policing cybercrime: emerging trends and future challenges. In T. Newburn (Ed.), *Handbook of Policing*. London: Routledge.

Jin, G. Z., & Kato, A. (2006). Price, quality, and reputation: evidence from an online field experiment. *RAND Journal of Economics, 37*(4), 983-1005. doi:10.1111/j.1756-2171.2006.tb00067.x

Johnson, N. D., & Mislin, A. A. (2011). Trust games: A meta-analysis. *Journal of Economic Psychology, 32*(5), 865-889. doi:10.1016/j.joep.2011.05.007

Johnston, L. (1992). *The Rebirth of Private Policing*. London: Routledge.

Johnston, L. E. S. (1996). What is vigilantism? *, 36*(2), 220-236. doi:10.1093/oxfordjournals.bjc.a014083

Jones, T., & Newburn, T. (1998). *Private Security and Public Policing*. Oxford: Oxford University Press.

Jones, T., Newburn, T., & Reiner, R. (2017). Policing and the police. In A. Liebling, S. Maruna, & L. McAra (Eds.), *The Oxford Handbook of Criminology*: Oxford University Press.

Kigerl, A. (2018). Profiling Cybercriminals: Topic Model Clustering of Carding Forum Member Comment Histories. *Social Science Computer Review, 36*(5), 591-609. doi:10.1177/0894439317730296

Krebs, B. (2015). *Spam Nation: The Inside Story of Organized Cybercrime-From Global Epidemic to Your Front Door*: Sourcebooks.

Kreps, D. M., Buckley, P. J., & Michie, J. (2003). *Corporate culture and economic theory*.

Krippendorff, K. (2013). *Content analysis : an introduction to its methodology* (3rd ed.). Los Angeles ; London: SAGE.

Krishnasamy, K., & Stoner, S. (2016). *Trading Faces: A Rapid Assessment on the use of Facebook to Trade Wildlife in Peninsular Malaysia*. Retrieved from TRAFFIC Petaling Jaya, Selangor, Malaysia.: https://www.traffic.org/site/assets/files/2434/trading-faces-facebook-malasia.pdf. [March 4th 2020]

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade - An analysis of the size, scope and the role of the Netherlands*. Retrieved from WODC, Ministerie van Veiligheid en Justitie: https://www.rand.org/pubs/research_reports/RR1607.html. [June 4th 2020]

Ladegaard, I. (2018). We Know Where You Are, What You Are Doing and We Will Catch You. *The British Journal of Criminology, 58*(2), 414-433. doi:10.1093/bjc/azx021

Ladegaard, I. (2019). "I Pray That We Will Find a Way to Carry on This Dream": How a Law Enforcement Crackdown United an Online Community. *Critical sociology, 45*(4-5), 631-646. doi:10.1177/0896920517735670

Lafky, J. (2014). Why do people rate? Theory and evidence on online ratings. *Games and Economic Behavior, 87*(C), 554-570. doi:10.1016/j.geb.2014.02.008

Lavorgna, A. (2013). *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes.* (PhD), University of Trento, Italy.

Lavorgna, A. (2014a). Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics. *Trends in Organized Crime, 17*(4), 250-270. doi:10.1007/s12117-014-9226-8

Lavorgna, A. (2014b). Wildlife trafficking in the Internet age. *Crime Science, 3*(1). doi:10.1186/s40163-014-0005-2

Lavorgna, A. (2015a). The online trade in counterfeit pharmaceuticals: New criminal opportunities, trends and challenges. *European Journal of Criminology, 12*(2), 226-241. doi:10.1177/1477370814554722

Lavorgna, A. (2015b). The Social Organization of Pet Trafficking in Cyberspace. *European Journal on Criminal Policy and Research, 21*(3), 353-370. doi:10.1007/s10610-015-9273-y

Lavorgna, A. (2016). How the use of the internet is affecting drug trafficking practices. In EMCDDA (Ed.), *The Internet and drug markets* (pp. 85-92). Luxembourg: Publications Office of the European Union.

Lavorgna, A. (2018). Online wildlife trafficking: a criminological perspective. *Evidence for Action 2018 - Research to address the Illegal Wildlife Trade.* Retrieved from https://www.youtube.com/watch?v=WcNLFv-S1L4. [May 21st 2021]

Lavorgna, A., Middleton, S. E., Pickering, B., & Neumann, G. (2020). FloraGuard: Tackling the Online Illegal Trade in Endangered Plants Through a Cross-Disciplinary ICT-Enabled Methodology. *Journal of Contemporary Criminal Justice, 36*(3), 428-450. doi:10.1177/1043986220910297

Lavorgna, A., & Sajeva, M. (2020). Studying Illegal Online Trades in Plants: Market Characteristics, Organisational and Behavioural Aspects, and Policing Challenges. *European Journal on Criminal Policy and Research*. doi:10.1007/s10610-020-09447-2

Leppänen, A., & Kankaanranta, T. (2020). Co-production of cybersecurity: a case of reported data system break-ins. *Police Practice & Research, 21*(1), 78-94. doi:10.1080/15614263.2018.1525382

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016a). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change, 67*(1), 39-53. doi:10.1007/s10611-016-9663-1

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016b). A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*(1), 21-37. doi:10.1007/s10611-016-9662-2

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263-280. doi:10.1080/01639625.2015.1012409

Levitt, S. D., & List, J. A. (2007). What Do Laboratory Experiments Measuring Social Preferences Reveal About the Real World? *Journal of Economic Perspectives, 21*(2), 153-174. doi:10.1257/jep.21.2.153

Levitt, S. D., & List, J. A. (2008). Homo economicus Evolves. *Science, 319*(5865), 909-910. doi:10.1126/science.1153640

Lewandowski, C., Carter, J. G., & Campbell, W. L. (2017). The role of people in information-sharing: perceptions from an analytic unit of a regional fusion center. *Police Practice and Research, 18*(2), 174-193. doi:10.1080/15614263.2016.1250631

Li, L. (2010). Reputation, Trust, and Rebates: How Online Auction Markets Can Improve Their Feedback Mechanisms. *Journal of Economics & Management Strategy, 19*(2), 303-331. doi:10.1111/j.1530-9134.2010.00253.x

Lin, H. (2016). *Attribution of Malicious Cyber Incidents - From soup to nuts*. Retrieved from Hoover Working Group on National Security, Technology, and Law, Aegis paper Series No 1607: https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf. [July 7th 2021]

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime, 13*(2), 71-94. doi:10.1080/17440572.2012.674183

Lusthaus, J. (2018). *Industry of anonymity : inside the business of cybercrime*. Cambridge, Massachusetts: Harvard University Press.

Mackey, T. K., & Liang, B. A. (2013). Global reach of direct-to-consumer advertising using social media for illicit online drug sales. *Journal of medical Internet research, 15*(5), e105. doi:10.2196/jmir.2610

Maguire, M., Morgan, R., & Reiner, R. (2012). *The Oxford handbook of criminology* (5th ed.). Oxford: Oxford University Press.

Malm, A., & Bichler, G. (2011). Networks of Collaborating Criminals: Assessing the Structural Vulnerability of Drug Markets. *The journal of research in crime and delinquency, 48*(2), 271-297. doi:10.1177/0022427810391535

Margulies, J. D., Bullough, L. A., Hinsley, A., Ingram, D. J., Cowell, C., Goettsch, B., . . . Phelps, J. (2019). Illegal wildlife trade and the persistence of "plant blindness". *Plants, People, Planet, 1*(3), 173-182. doi:10.1002/ppp3.10053

Martin, Cunliffe, J., Decary-Hetu, D., & Aldridge, J. (2018a). Effect of restricting the legal supply of prescription opioids on buying through online illicit marketplaces: interrupted time series analysis. *BMJ, 361*, k2270. doi:10.1136/bmj.k2270

Martin, Senni, C., & D'Cruze, N. C. (2018b). Trade in wild-sourced African grey parrots: Insights via social media. *Global Ecology and Conservation, 15*, e00429. doi:10.1016/j.gecco.2018.e00429

Matthews, B., & Ross, L. (2010). *Research methods : a practical guide for the social sciences*. Harlow ; New York: Pearson Longman.

Maxwell, S. R. J., & Webb, D. J. (2008). Internet pharmacy: a web of mistrust? *British Journal of Clinical Pharmacology, 66*(2), 196-198. doi:10.1111/j.1365-2125.2008.03215.x

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Isjlp, 4*, 543.

McLaughlin, E., & Newburn, T. (2010). *The SAGE handbook of criminological theory*. London: SAGE.

Mell, A. (2012). Reputation in the Market for Stolen Data. *IDEAS Working Paper Series from RePEc*.

Melnik, M., & Alm, J. (2002). Does a seller's ecommerce reputation matter? Evidence from Ebay auctions. *The Journal of Industrial Economics, 50*(3), 337-349.

Microsoft. (2021). Digital Crimes Unit: Leading the fight against cybercrime. Retrieved from https://news.microsoft.com/on-the-issues/2021/04/15/how-microsofts-digital-crimes-unit-fights-cybercrime/. [July 7th 2021]

Milan, S., & Hintz, A. (2013). Networked Collective Action and the Institutionalized Policy Debate: Bringing Cyberactivism to the Policy Arena? *Policy & Internet, 5*(1), 7-26. doi:10.1002/poi3.20

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis : an expanded sourcebook* (2nd ed.). Thousand Oaks, Calif. ; London: Sage.

Milgrom, P. R., North, D. C., & Weingast*, B. R. (1990). The role of institutions in the revival of trade: the law merchant, private judges, and the champagne fairs. *Economics & Politics, 2*(1), 1-23. doi:10.1111/j.1468-0343.1990.tb00020.x

Mireault, C., Ouellette, V., Décary-Hétu, D., Crispino, F., & Broséus, J. (2016). Potentiel criminalistique de l'étude du trafic de drogues au Canada à partir des données collectées sur les cryptomarchés. *Canadian Society of Forensic Science Journal, 49*(4), 161-175. doi:10.1080/00085030.2016.1189229

Moreto, W. D., & Clarke, R. V. (2013). Script analysis of the transnational illegal market in endangered species - dream and reality. In B. LeClerc & R. Wortley (Eds.), *Cognition and Crime: Offender Decision Making and Script Analyses*. New York: Routledge.

Morgan, D. L. (1993). Qualitative Content Analysis: A Guide to Paths not Taken. *Qualitative Health Research, 3*(1), 112-121. doi:10.1177/104973239300300107

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict Management in Illicit Drug Cryptomarkets. *International Criminal Justice Review, 27*(4), 237-254. doi:10.1177/1057567717709498

Moshier, A., Steadman, J., & Roberts, D. L. (2019). Network analysis of a stakeholder community combatting illegal wildlife trade. *Conservation Biology, 33*(6), 1307-1317. doi:10.1111/cobi.13336

Moyle, L., Childs, A., Coomber, R., & Barratt, M. J. (2019). #Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy, 63*(January 2019), 101-110.

Munksgaard, R., & Demant, J. (2016). Mixing politics and crime – The prevalence and decline of political discourse on the cryptomarket. *International Journal of Drug Policy, 35*, 77-83. doi:10.1016/j.drugpo.2016.04.021

Neuendorf, K. A. (2016). *The content analysis guidebook* (Second ed.). Los Angeles: SAGE.

Norbutas, L. (2018). Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network. *International Journal of Drug Policy, 56*, 92-3959.

Norbutas, L. (2020). *Trust on the Dark Web: An analysis of illegal online drug markets.* (PhD thesis), Utrecht University,

Noussair, C., & Tucker, S. (2014). *A collection of surveys on market experiments*. Chichester: Wiley Blackwell.

Nurse, A. (2013). Privatising the green police: the role of NGOs in wildlife law enforcement. *An Interdisciplinary Journal, 59*(3), 305-318. doi:10.1007/s10611-013-9417-2

Olive, D. J. (2017). *Linear regression*. Cham, Switzerland: Springer.

Oliveira, I. S. (2014). Catch Me If You Can: or how policy networks help tackle the crime-terror nexus. *Global Crime: Transnational Organized Crime and Terrorism: Different Peas, Same Pod?, 15*(3-4), 219-240. doi:10.1080/17440572.2014.937429

Paquet-Clouston, M., Décary-Hétu, D., & Bilodeau, O. (2017). Cybercrime is whose responsibility? A case study of an online behaviour system in crime. *Global Crime, 19*(1), 1-21. doi:10.1080/17440572.2017.1411807

Paquet-Clouston, M., Decary-Hetu, D., & Morselli, C. (2018). Assessing market competition and vendors' size and scope on AlphaBay. *Int J Drug Policy, 54*, 87-98. doi:10.1016/j.drugpo.2018.01.003

Payne, B., & Hadzhidimova, L. (2020). Disciplinary and Interdisciplinary Trends in Cybercrime Research: An Examination. *International Journal of Cyber Criminology, 14*(1), 81-105.

Perez-Truglia, R. (2018). Markets, trust and cultural biases: evidence from eBay. *Journal of Behavioral and Experimental Economics, 72*, 17-27. doi:10.1016/j.socec.2017.11.004

Petersen, K. L. (2008). Risk, responsibility and roles redefined: is counterterrorism a corporate responsibility? *Cambridge Review of International Affairs, 21*(3), 403-420. doi:10.1080/09557570802253633

Pets4Homes. (2020). Terms & Conditions. Retrieved from https://www.pets4homes.co.uk/terms/#standards. [March 31st 2020]

Phelps, A., & Watt, A. (2014). I shop online - recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation, 11*(4), 261.

Pink, G., & White, R. D. (2016). *Environmental crime and collaborative state intervention*. Basingstoke, Hampshire: Palgrave Macmillan.

Pollach, I. (2007). What's wrong with online privacy policies? *Communications of the ACM, 50*(9), 103-108.

Potter, W. J., & Levine-Donnerstein, D. (1999). Rethinking validity and reliability in content analysis. *Journal of Applied Communication Research, 27*(3), 258-284. doi:10.1080/00909889909365539

Poulsen, K. (2011). *Kingpin - how one hacker took over the billion-dollar cybercrime underground*. New York: Crown Publishers.

Preloved. (2011). Buying and carrying for a tortoise. Retrieved from https://www.preloved.co.uk/blog/animals/buying-and-caring-for-a-tortoise/. [March 27th 2020]

Preloved. (2015a). Preloved listing guidelines. Retrieved from https://www.preloved.co.uk/guidelines. [March 27th 2020]

Preloved. (2015b). Press release - Preloved Bans The Sale of Ivory. Retrieved from https://www.preloved.co.uk/press/release/1563/preloved-bans-the-sale-of-ivory.html. [March 27th 2020]

Preloved. (2015c). Tortoise breed list and care guide. Retrieved from https://www.preloved.co.uk/blog/animals/tortoise-breed-list-care-guide/. [March 31st 2020]

Preloved. (2015d). Why Preloved does not allow the sale of ivory. Retrieved from https://www.preloved.co.uk/blog/preloved-news/preloved-not-allow-sale-ivory/. [March 27th 2020]

Preloved. (2017). CoP17: CITES updates for endangered species. Retrieved from https://www.preloved.co.uk/blog/animals/cop17-cites-updates-for-endangered-species/. [March 27th 2020]

Preloved. (2020). Selling endangered species. Retrieved from https://www.preloved.co.uk/animals/cites. [March 27th 2020]

Prenzler, T. (2006). Private investigators. In M. Gill (Ed.), *The handbook of security* (pp. 423-437). Basingstoke: Palgrave.

Putnam, R. D., Leonardi, R., & Nanetti, R. (1993). *Making democracy work : civic traditions in modern Italy*. Princeton, N.J. ; Chichester: Princeton University Press.

Rabby, F., & Shahriar, Q. (2016). Non-Neutral and Asymmetric Effects of Neutral Ratings: Evidence From eBay. *Managerial and Decision Economics, 37*(2), 95-105. doi:10.1002/mde.2696

Rawlings, P. (1995). The idea of policing: A history. *Policing & society, 5*(2), 129-149. doi:10.1080/10439463.1995.9964718

Reiley, D. (2015). *Handbook of Experimental Economic Methodology*: Oxford University Press.

Reppetto, T. A. (1976). Crime Prevention and the Displacement Phenomenon. *Crime & Delinquency, 22*(2), 166-177. doi:10.1177/001112877602200204

Resnick, P., & Zeckhauser, R. (2002). Trust among strangers in Internet transactions: empirical analysis of eBay's reputation system. In M. R. Baye (Ed.), *The economics of the Internet and e-commerce*. Amsterdam: Elsevier Science.

Resnick, P., Zeckhauser, R., Swanson, J., & Lockwood, K. (2003). The Value of Reputation on eBay: A Controlled Experiment. *IDEAS Working Paper Series from RePEc*.

Rivlin, A. (1974). Social experiments: their uses and limitations. *Monthly Labor Review, 97*(6), 28.

Roth, A. E. (1993). The Early History of Experimental Economics. *Journal of the History of Economic Thought, 15*(2), 184-209. doi:10.1017/S1053837200000936

Roth, A. E. (2007). Repugnance as a Constraint on Markets. *Journal of Economic Perspectives, 21*(3), 37-58. doi:10.1257/jep.21.3.37

Runhovde, S. R. (2017). Taking the Path of Least Resistance? Decision-Making in Police Investigations of Illegal Wildlife Trade. *Policing: A Journal of Policy and Practice, 11*(1), 87-102. doi:10.1093/police/paw026

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). Los Angeles ; London: SAGE.

Sandberg, S. (2012). The Importance of Culture for Cannabis Markets. *British Journal of Criminology, 52*(6), 1133-1151. doi:10.1093/bjc/azs031

Sarre, R., Lau, L. Y.-C., & Chang, L. Y. C. (2018). Responding to cybercrime: current trends. *Police Practice and Research: Responding to Cybercrime: Current Trends, 19*(6), 515-518. doi:10.1080/15614263.2018.1507888

Scammell, L., & Bo, A. (2016). Online supply of medicines to illicit drug markets: situation and responses. In EMCDDA (Ed.), *The Internet and drug markets* (pp. 107-114). Lisbon: EMCDDA.

Schelling, T. C. (1960). *The strategy of conflict*. Cambridge, Mass.: Harvard University Press.

Schelling, T. C. (1984). Strategic analysis and social problems. In T. C. Schelling (Ed.), *Choice and consequence. Perspectives of an errant economist.* Cambridge, Massachusetts: Harvard University Press.

Schreier, M. (2012). *Qualitative content analysis in practice*. London: SAGE.

Serious Crime Act, (2015).

Shore, M., Du, Y., & Zeadally, S. (2011). A Public-Private Partnership Model for National Cybersecurity. *Policy & Internet, 3*(2), 168-190. doi:10.2202/1944-2866.1114

Siegel, S., & Fouraker, L. E. (1960). *Bargaining and group decision making : experiments in bilateral monopoly*. New York: McGraw-Hill.

Soska, K., & Christin, N. (2015, August 12–14). *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem.* Paper presented at the Proceedings of the 24th USENIX Security Symposium, Washington, D.C., USA.

South, N., & Wyatt, T. (2011). Comparing Illicit Trades in Wildlife and Drugs: An Exploratory Study. *Deviant Behavior, 32*(6), 538-561. doi:10.1080/01639625.2010.483162

Steinfeld, N. (2016). "I agree to the terms and conditions":(How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior, 55*, 992-1000.

Sugiura, L. (2018). *Respectable deviance and purchasing medicine online : opportunities and risks for consumers*. Cham, Switzerland: Palgrave Macmillan.

Sugiura, L., Pope, C., & Webber, C. (2012, June 22-24). *Buying unlicensed slimming drugs from the Web: a virtual ethnography.* Paper presented at the 4th Annual ACM Web Science Conference, Evanston, Illinois, USA.

Swanstrom, N. (2007). The Narcotics Trade: A Threat to Security? National and Transnational Implications. *Global Crime, 8*(1), 1-25. doi:10.1080/17440570601121829

Thanki, D., & Frederick, B. (2016). *Social media and drug markets*. The internet and drug markets. Publications Office of the European Union. Luxembourg.

The Economist. (2014). The Amazons of the dark net. Retrieved from https://www.economist.com/international/2014/11/01/the-amazons-of-the-dark-net. [April 7th 2020]

The Economist. (2021). Opioid deaths in America reached new highs in the pandemic. *Daily chart.* Retrieved from https://www.economist.com/graphic-detail/2021/03/30/opioid-deaths-in-america-reached-new-highs-in-the-pandemic?utm_campaign=editorial-social&utm_medium=social-organic&utm_source=linkedin. [April 14th 2021]

Tolbert, C. M. (2005). Minding Our Own Business: Local Retail Establishments and the Future of Southern Civic Community. *Social Forces, 83*(4), 1309-1328. doi:10.1353/sof.2005.0084

TRAFFIC. (2019). *Wildlife cyber crime trends in China - online monitoring results 2017-2018*. Retrieved from https://www.traffic.org/publications/reports/wildlife-cybercrime-trends-in-china/. [March 24th 2020]

TRAFFIC WWF IFAW. (2017). *Wildlife-friendly online trade 2017: a harmonised policy for e-commerce and social media companies*. Retrieved from https://c402277.ssl.cf1.rackcdn.com/publications/924/files/original/WWF_TRAFFIC_and_IFAW_Wildlife_Friendly_Policy_2017.pdf?1510328189. [March 4th 2020]

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254-268.

Turow, J., Hennessy, M., & Bleakley, A. (2008). Consumers' understanding of privacy rules in the marketplace. *Journal of consumer affairs, 42*(3), 411-424.

Twitter. (2019). Illegal or certain regulated goods or services. Retrieved from https://help.twitter.com/en/rules-and-policies/regulated-goods-services. [April 5th 2020]

United Nations Convention against Transnational Organized Crime, (2000).

United Nations Environmental Programme, & Interpol. (2016). *The rise of environmental crime - a growing threat to national resources, peace, development and security*. Retrieved from https://wedocs.unep.org/handle/20.500.11822/7662?show=full. [February 1st 2021]

United Nations Office at Vienna. (2020). United Nations Office on Drugs and Crime (UNODC). Retrieved from https://www.unov.org/unov/en/unodc.html. [May 27th 2020]

15-1815-cr United States of America v. Ross William Ulbricht, United States Court of Appeals for the Second Circuit 139 (2016).

United States of America Department of Justice. (2014a). Dozens of online markets seized pursuant to forfeiture complaint filed in Manhattan Federal Court in conjunction with the arrest of the operator of Silk Road 2.0. Retrieved from https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/dozens-of-online-dark-markets-seized-pursuant-to-forfeiture-complaint-filed-in-manhattan-federal-court-in-conjunction-with-the-arrest-of-the-operator-of-silk-road-2.0. [27th February 2019]

United States of America Department of Justice. (2014b). Montgomery County pair charged in eBay scam. Retrieved from https://www.fbi.gov/contact-us/field-offices/philadelphia/news/press-releases/montgomery-county-pair-charged-in-ebay-scam. [27th February 2019]

United States of America Department of Justice. (2015). Bitcoin exchanger sentenced in Manhattan Federal Court to four years in prison for selling nearly $1 million in bitcoins for drug buys on Silk Road. Retrieved from https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/bitcoin-exchanger-sentenced-in-manhattan-federal-court-to-four-years-in-prison-for-selling-nearly-1-million-in-bitcoins-for-drug-buys-on-silk-road. [27th February 2019]

United States of America Department of Justice. (2016a). ICYEAGLE, a darkweb vendor of stolen information, sentenced to Federal prison. Retrieved from https://www.justice.gov/usao-ndga/pr/icyeagle-dark-web-vendor-stolen-information-sentenced-federal-prison. [27th February 2019]

United States of America Department of Justice. (2016b). Key player in 'Silk Road 2.0' sentenced to 8 years in prison. Retrieved from https://www.justice.gov/usao-wdwa/pr/key-player-silk-road-20-sentenced-eight-years-prison. [27th February 2019]

United States of America Department of Justice. (2016c). New Orleans man sentenced to 41 months for manufacturing and selling more than $1 million in counterfeit coupons on SIlk Road. Retrieved from https://www.justice.gov/usao-edla/pr/new-orleans-man-sentenced-41-months-manufacturing-and-selling-more-1-million. [27th February 2019]

United States of America Department of Justice. (2018a). Darkweb administrator sentenced to 20 years for narcotics trafficking and money laundering. Retrieved from https://www.justice.gov/usao-sdfl/pr/dark-web-administrator-sentenced-20-years-prison-narcotics-trafficking-and-money. [27th February 2019]

United States of America Department of Justice. (2018b). Operation Darkness Fall results in arrest of one of the most prolific dark net fentanyl vendors in the world. Retrieved from https://www.justice.gov/usao-ndoh/pr/operation-darkness-falls-results-arrest-one-most-prolific-dark-net-fentanyl-vendors. [27th February 2019]

UNODC. (2012a). *Wildlife and forest crime analytic toolkit*. Retrieved from http://www.unodc.org/documents/Wildlife/Toolkit_e.pdf. [May 27th 2020]

UNODC. (2012b). *World Drug Report*. Retrieved from https://www.unodc.org/documents/data-and-analysis/WDR2012/WDR_2012_web_small.pdf. [May 27th 2020]

UNODC. (2013). *World Drug Report*. Retrieved from https://www.unodc.org/unodc/secured/wdr/wdr2013/World_Drug_Report_2013.pdf. [May 27th 2020]

UNODC. (2014). *World Drug Report*. Retrieved from https://www.unodc.org/documents/wdr2014/World_Drug_Report_2014_web.pdf. [May 27th 2020]

UNODC. (2015). *World Drug Report*. Retrieved from https://www.unodc.org/documents/wdr2015/World_Drug_Report_2015.pdf. [May 27th 2020]

UNODC. (2016a). *World Drug Report*. Retrieved from https://www.unodc.org/doc/wdr2016/WORLD_DRUG_REPORT_2016_web.pdf. [May 27th 2020]

UNODC. (2016b). *World Wildlife Crime Report - Trafficking in protected species*. Retrieved from https://www.unodc.org/documents/data-and-analysis/wildlife/World_Wildlife_Crime_Report_2016_final.pdf. [May 27th 2020]

UNODC. (2017a). *World Drug Report 1 – Executive summary conclusions and policy implications*. Retrieved from https://www.unodc.org/wdr2017/field/Booklet_1_EXSUM.pdf. [May 27th 2020]

UNODC. (2017b). *World Drug Report 2 – Global overview of drug demand and supply latest trends, cross-cutting issues*. Retrieved from https://www.unodc.org/wdr2017/field/Booklet_2_HEALTH.pdf. [May 27th 2020]

UNODC. (2017c). *World Drug Report 4 – Market analysis of synthetic drugs amphetamine-type stimulants, new psychoactive substances*. Retrieved from https://www.unodc.org/wdr2017/field/Booklet_4_ATSNPS.pdf. [May 27th 2020]

UNODC. (2018a). *Guide on drafting legislation to combat wildlife crime*. Retrieved from https://www.unodc.org/documents/Wildlife/Legislative_Guide.pdf. [May 27th 2020]

UNODC. (2018b). *World Drug Report 1 – Executive summary conclusions and policy implications*. Retrieved from https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_1_EXSUM.pdf. [May 27th 2020]

UNODC. (2018c). *World Drug Report 2 – Global overview of drug demand and supply latest trends, cross-cutting issues*. Retrieved from https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_2_GLOBAL.pdf. [May 27th 2020]

UNODC. (2018d). *World Drug Report 3 – Analysis of drug markets opiates, cocaine, cannabis, synthetic drugs*. Retrieved from https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_3_DRUG_MARKETS.pdf. [May 27th 2020]

UNODC. (2018e). *World Drug Report 4 – Drugs and age, drugs and associated issues among young people and older people*. Retrieved from https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_4_YOUTH.pdf. [May 27th 2020]

UNODC. (2018f). *World Drug Report 5 – Women and drugs, drug use, drug supply and their consequences*. Retrieved from https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_5_WOMEN.pdf. [May 27th 2020]

UNODC. (2019a). *World Drug Report 1 - Executive Summary Conclusions and policy implications*. Retrieved from https://wdr.unodc.org/wdr2019/prelaunch/WDR19_Booklet_1_EXECUTIVE_SUMMARY.pdf. [May 27th 2020]

UNODC. (2019b). *World Drug Report 2 - Global overview of drug demand and supply*. Retrieved from https://wdr.unodc.org/wdr2019/prelaunch/WDR19_Booklet_2_DRUG_DEMAND.pdf. [May 27th 2020]

UNODC. (2019c). *World Drug Report 4 - Stimulants*. Retrieved from https://wdr.unodc.org/wdr2019/prelaunch/WDR19_Booklet_4_STIMULANTS.pdf. [May 27th 2020]

UNODC. (2020a). Activity areas. Retrieved from https://www.unodc.org/images/about-unodc/activity-areas_1100x1251px.jpg. [May 27th 2020]

UNODC. (2020b). Topics. Retrieved from https://www.unodc.org/unodc/en/topics.html. [May 27th 2020]

UNODC. (2020c). *World Drug Report 1 - Executive summary, impact of covid-19, policy implication*. Retrieved from https://wdr.unodc.org/wdr2020/en/exsum.html. [May 27th 2020]

UNODC. (2020d). *World Drug Report 4 - Cross-cutting issues: evolving trends and new challenges*. Retrieved from https://wdr.unodc.org/wdr2020/en/cross-cutting.html. [May 27th 2020]

UNODC. (2020e). *World Wildlife Crime Report - Trafficking in protected species*. Retrieved from https://www.unodc.org/documents/data-and-analysis/wildlife/2020/World_Wildlife_Report_2020_9July.pdf. [May 27th 2020]

UNODC. (2021a). Demand and Consumption. *E4J University Module Series: Wildlife Crime.* Retrieved from https://www.unodc.org/e4j/en/wildlife-crime/module-1/key-issues/demand-and-consumption.html. [February 1st 2021]

UNODC. (2021b). Drug trafficking. Retrieved from https://www.unodc.org/unodc/en/drug-trafficking/index.html. [February 1st 2021]

UNODC. (2021c). *World Drug Report 2021 - Executive Summary Policy Implications*. Retrieved from https://www.unodc.org/res/wdr2021/field/WDR21_Booklet_1.pdf. [June 17th 2021]

UNODC. (2021d). *World Drug Report 2021 - Global overview: drug demand drug suplly*. Retrieved from https://www.unodc.org/res/wdr2021/field/WDR21_Booklet_2.pdf. [June 17th 2021]

US Endangered Species Act, (1973).

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. doi:10.1016/j.drugalcdep.2017.01.004

Van Buskirk, J., Roxburgh, A., Farrell, M., & Burns, L. (2014). The closure of the Silk Road: what has this meant for online drug trading? *Addiction, 109*(4), 517-518. doi:10.1111/add.12422

Van Hout, M. C., & Bingham, T. (2013). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy, 24*(5), 385-391. doi:10.1016/j.drugpo.2013.01.005

Veríssimo, D., & Wan, A. K. Y. (2019). Characterizing efforts to reduce consumer demand for wildlife products. *Conservation Biology, 33*(3), 623-633. doi:10.1111/cobi.13227

Vila, T., Greenstadt, R., & Molnar, D. (2003). *Why we can't be bothered to read privacy policies models of privacy economics as a lemons market.* Paper presented at the Proceedings of the 5th international conference on Electronic commerce.

Viollaz, J., Graham, J., & Lantsman, L. (2018). Using script analysis to understand the financial crimes involved in wildlife trafficking. *An Interdisciplinary Journal, 69*(5), 595-614. doi:10.1007/s10611-017-9725-z

Von Neumann, J., & Morgenstern, O. (2007). *Theory of games and economic behavior* (60th anniversary ed. ed.). Princeton, N.J. ; Woodstock: Princeton University Press.

Wakefield, A. (2003). *Selling security : the private policing of public space.* Willan, Cullompton.

Wakefield, A., & Button, M. (2014). Private Policing in Public Spaces In M. D. Reisig & R. J. Kane (Eds.), *The Oxford Handbook of Police and Policing*: Oxford University Press.

Wall, D. (1998). Catching Cybercriminals: Policing the Internet. *International Review of Law, Computers & Technology, 12*(2), 201-218. doi:10.1080/13600869855397

Wall, D. (2007a). *Cybercrime : the transformation of crime in the information age*. Cambridge: Polity.

Wall, D. (2007b). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. *Police Practice and Research, 8*(2), 183-205. doi:10.1080/15614260701377729

Wall, D. S., & Williams, M. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology & criminal justice, 7*(4), 391-415.

Wallen, K. E., & Daut, E. F. (2018). The challenge and opportunity of behaviour change methods and frameworks to reduce demand for illegal wildlife.(Report). *Nature Conservation, 26*(26), 55. doi:10.3897/natureconservation.26.22725

Warren, S., Oxburgh, G., Briggs, P., & Wall, D. (2017, July 9 - 14). *How Might Crime-Scripts Be Used to Support the Understanding and Policing of Cloud Crime?* Paper presented at the HCI International, Vancouver, BC, Canada.

WCO. (2009). *International operation combats the online supply of counterfeit and illegal medicines*. Retrieved from http://www.wcoomd.org/en/media/newsroom/2009/november/international-operation-combats-the-online-supply-of-counterfeit-and-illegal-medicines.aspx. [May 24th 2020]

WCO. (2010a). *Strong public safety focus of global operation targeting counterfeit and illegal medicines traded online*. Retrieved from http://www.wcoomd.org/en/media/newsroom/2010/october/strong-public-safety-focus-of-global-operation-targeting-counterfeit-and-illegal-medicines-traded-online.aspx. [May 24th 2020]

WCO. (2010b). *WCO News*. Retrieved from http://www.wcoomd.org/-/media/wco/public/global/pdf/media/wco-news-magazines/wco_news_61.pdf. [May 24th 2020]

WCO. (2011). *Global operation strikes at online supply of illegal and counterfeit medicines worldwide*. Retrieved from http://www.wcoomd.org/en/media/newsroom/2011/september/global-operation-strikes-at-online-supply-of-illegal-and-counterfeit-medicines-worldwide.aspx. [May 24th 2020]

WCO. (2012a). *Annual report 2011-2012*. Retrieved from http://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/annual-reports/annual-report-2011_2012.pdf. [May 24th 2020]

WCO. (2012b). *Tackling organized crime networks behind global crackdown on illicit online pharmacies*. Retrieved from http://www.wcoomd.org/en/media/newsroom/2012/october/pangea-v.aspx. [May 24th 2020]

WCO. (2012c). *WCO News*. Retrieved from http://www.wcoomd.org/-/media/wco/public/global/pdf/media/wco-news-magazines/wco_news69_oct-2012_en.pdf. [May 24th 2020]

WCO. (2013a). *Annual report 2012-2013*. Retrieved from http://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/annual-reports/annual-report-2012_2013.pdf. [May 24th 2020]

WCO. (2013b). *International operation targets online sale of illicit medicines*. Retrieved from http://www.wcoomd.org/en/media/newsroom/2013/june/pangea-vi-international-operation.aspx. [May 24th 2020]

WCO. (2014a). *Illicit trade report*. Retrieved from http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/illicit-trade-report/itr_2014_en.pdf?db=web. [May 24th 2020]

WCO. (2014b). *Thousands of illicit online pharmacies shut down in global operation targeting fake medicines*. Retrieved from http://www.wcoomd.org/en/media/newsroom/2014/may/thousands-of-illicit-online-pharmacies-shut-down-in-global-operation-targeting-fake-medicines.aspx. [May 24th 2020]

WCO. (2015a). *Millions USD worth illicit medicines seized in global operation*. Retrieved from http://www.wcoomd.org/en/media/newsroom/2015/june/millions-usd-worth-illicit-medicines-seized-in-global-operation.aspx. [May 24th 2020]

WCO. (2015b). *WCO News*. Retrieved from http://www.wcoomd.org/-/media/wco/public/global/pdf/media/wco-news-magazines/wconews_78_uk.pdf. [May 24th 2020]

WCO. (2016a). *French Customs seizes hundreds of archaeological objects and endangered wildlife products* Retrieved from http://www.wcoomd.org/en/media/newsroom/2016/february/french-customs-seizes-hundreds-of-archeological-objects-and-endangered-wildlife-products.aspx. [May 24th 2020]

WCO. (2016b). *WCO News*. Retrieved from http://www.wcoomd.org/-/media/wco/public/global/pdf/media/wco-news-magazines/wco_news_79.pdf. [May 24th 2020]

WCO. (2016c). *WCO participates in Operation Pangea IX against fake and illicit medicines* Retrieved from http://www.wcoomd.org/en/media/newsroom/2016/june/wco-participates-in-operation-pangea-ix-against-fake-and-illicit-medicines.aspx. [May 24th 2020]

WCO. (2018). *Illicit trade report*. Retrieved from http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/illicit-trade-report/itr_2018_en.pdf?db=web. [May 24th 2020]

WCO. (2019). *Wildlife trafficking: Organized crime hit hard by joint WCO-INTERPOL global enforcement operation*. Retrieved from http://www.wcoomd.org/en/media/newsroom/2019/july/wildlife-trafficking_organized-crime-hit-hard-by-joint-wco_interpol-global-enforcement-operation.aspx. [May 24th 2020]

WCO. (2020a). *COVID-19 Urgent Notice: counterfeit medical supplies and introduction of export controls on personal protective equipment*. Retrieved from http://www.wcoomd.org/en/media/newsroom/2020/march/covid_19-urgent-notice-counterfeit-medical-supplies. [May 24th 2020]

WCO. (2020b). Discover the WCO - Customs role. Retrieved from https://clikc.wcoomd.org/mod/scorm/player.php?a=3832&currentorg=articulate_rise&scoid=34276. [May 24th 2020]

WCO. (2020c). Discover the WCO - History. Retrieved from https://clikc.wcoomd.org/mod/scorm/player.php?a=3832&currentorg=articulate_rise&scoid=34276. [May 24th 2020]

WCO. (2020d). Discover the WCO - Key activities. Retrieved from https://clikc.wcoomd.org/mod/scorm/player.php?a=3832&currentorg=articulate_rise&scoid=34276. [May 24th 2020]

WCO. (2020e). Discover the WCO - Membership. Retrieved from https://clikc.wcoomd.org/mod/scorm/player.php?a=3832&currentorg=articulate_rise&scoid=34276. [May 24th 2020]

Webb, E. J. (1966). *Unobtrusive measures : nonreactive research in the social sciences*. Chicago: Rand McNally.

Weber, R. P. (1990). *Basic content analysis* (2nd ed.). Newbury Park ; London: Sage.

Webster, M., & Sell, J. (2007). *Laboratory experiments in the social sciences*. Amsterdam ; Oxford: Academic Press/Elsevier.

WeChat. (2015). Acceptable use policy. Retrieved from https://www.wechat.com/en/acceptable_use_policy.html. [April 4th 2020]

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in conflict and terrorism, 39*(3), 195-206. doi:10.1080/1057610X.2015.1119546

WhatsApp. (2019). Commerce Policy. Retrieved from https://www.whatsapp.com/legal/commerce-policy/. [April 4th 2020]

Wildlife and Countryside Act, (1981).

Williams, B. (1990). Formal structures and social reality. In D. Gambetta (Ed.), *Trust - Making and breaking cooperative relations* (pp. 3 - 13). Cambridge, Massachusetts: Basil Blackwell.

Williams, J. M. (2005). *Style : ten lessons in clarity and grace* (Eighth ed.). New York: Pearson Longman.

WJC. (2016a). Governments urged to support Vietnam in implementing Public Hearing recommendations. Retrieved from https://wildlifejustice.org/governments-urged-support-viet-nam-implementing-public-hearing-recommendations/. [March 27th 2020]

WJC. (2016b). Independent panel confirms that immediate action by the Vietnamese government is required to shut down wildlife trafficking networks in Vietnam. Retrieved from

https://wildlifejustice.org/independent-panel-confirms-immediate-action-vietnamese-government-required-shut-wildlife-trafficking-networks-viet-nam/. [March 27th 2020]

WJC. (2016c). *Operation Ambush*. Retrieved from https://wildlifejustice.org/operation-ambush-briefing-2016/. [March 27th 2020]

WJC. (2016d). Vietnam Public Hearing: Suggested recommendations from the audience and around the world. Retrieved from https://wildlifejustice.org/viet-nam-public-hearing-suggested-recommendations-audience-around-world/. [March 27th 2020]

WJC. (2017a). *Case study - Black business: illegal rhino horn trade dynamics in Nhi Khe, Viet Nam from a criminal perspective*. Retrieved from https://wildlifejustice.org/black-business-illegal-rhino-horn-viet-nam/. [March 27th 2020]

WJC. (2017b). *Operation Phoenix*. Retrieved from https://wildlifejustice.org/operation-phoenix-briefing-2018/. [March 27th 2020]

WJC. (2018a). *Operation Dragon Revealing new evidence of the scale of corruption and trafficking in the turtle and tortoise trade*. Retrieved from https://wildlifejustice.org/operation-dragon-new-evidence-of-the-scale-of-corruption-in-the-illegal-turtle-and-tortoise-trade-in-southeast-asia/. [March 27th 2020]

WJC. (2018b). *A Preliminary Analysis of Raw Rhino Horn Prices in Africa and Asia*. Retrieved from https://wildlifejustice.org/a-preliminary-analysis-of-raw-rhino-horn-prices-in-africa-and-asia-october-2018/. [March 27th 2020]

WJC. (2018c). *The prevalence of vulnerable South Asian freshwater turtles in the illegal trade*. Retrieved from https://wildlifejustice.org/the-prevalence-of-vulnerable-south-asian-freshwater-turtles-in-the-illegal-trade-october-2018/. [March 27th 2020]

WJC. (2020a). About Us. Retrieved from https://wildlifejustice.org/about-us. [March 27th 2020]

WJC. (2020b). Investigations. Retrieved from https://wildlifejustice.org/investigations/. [March 27th 2020]

WJC. (2020c). *Scaling up: The Rapid Growth in the Industrial Scale Trafficking of Pangolin Scales 2016-2019*. Retrieved from https://wildlifejustice.org/new-report-analyses-unprecedented-levels-of-pangolin-trafficking-urging-stakeholders-to-tackle-it-as-transnational-crime/. [March 27th 2020]

WJC. (2021). Joint operation with Thai and US law enforcement agencies leads to the arrest of suspected high-level wildlife trafficker. Retrieved from https://wildlifejustice.org/joint-operation-with-thai-and-us-law-enforcement-agencies-leads-to-the-arrest-of-suspected-high-level-wildlife-trafficker/ [June 21st 2021]

Wright, J. (2018). The Ethics of Online Illegal Wildlife Trade Research. *Evidence to Action 2018 - Research to address the illegal wildlife trade.* Retrieved from https://www.youtube.com/watch?v=WcNLFv-S1L4. [May 21st 2021]

Wright, J. (2019). Darknet Usage in the Illegal Wildlife Trade. *Tools and Guidance, Oxford Martin Programme on the Illegal Wildlife Trade, University of Oxford*. doi:10.31235/osf.io/fgr9d

Ying, F.-T., Yuan, H., & Lau, S.-L. (2014). Striving to Build Civic Communities. *Review of Religious and Chinese Society, 1*(1), 78-103. doi:10.1163/22143955-04102006

Yip, M., Shadbolt, N., & Webber, C. (2013a). Why Forums? An Empirical Analysis into the Facilitating Factors of Carding Forums. In (Vol. volume, pp. 453-462). Proceedings of the 5th Annual ACM Web Science Conference.

Yip, M., Webber, C., & Shadbolt, N. (2013b). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society, 23*(4), 516-539. doi:10.1080/10439463.2013.780227

Zhou, G., Zhuge, J., Du, K., & Lu, S. (2020). A market in Dream: the rapid development of anonymous cybercrime. *Mobile Networks and Applications, 25*, 259-270.

Appendices

Appendix A.1: Police interview topics

About you

1) Why did you choose to work for your organisation?
2) What does your current position entail?
3) Do you get to experience the policing of online illegal drug/wildlife trade as part of this position?
4) How long have you been working for your organisation?

Operational and strategic evolution

1) How long has your agency been involved in the policing of online illegal drug/wildlife trade?
2) What specific work has your organisation been involved in? (e.g. regulation, trade monitoring, arrests, seizures, platform content removal…)
3) During your time there, what major operational and strategic changes occurred as to your agency's approach to the policing of online illegal drug/wildlife trade?
4) What do you consider your agency's best strategic decision so far in that respect?

Policing of online illegal trade

1) Do you have thoughts or ideas about the best ways to reduce online illegal drug/wildlife trade?
2) Do you collaborate with any of the below for your work? If so which ones, for what purpose(s), how (e.g. meetings, emails, calls, trainings…), and how often?

- Other Police agencies whether regional or international
- Industry (e.g. private organisations, legal platforms …)
- Non-profits
- Inter-Governmental Organisations
- Policymakers
- Schools and Universities

3) How do the different entities' skills complement each other?
4) How often do you organise / attend inter-sector meetings about the policing of online illegal drug/wildlife trade? What are the other sectors represented? What is the main aim of these meetings?

Communication about online illegal trade policing

Do you ever publicly communicate, verbally or in writing, about online illegal drug/wildlife trade policing?

- What types of communications? (e.g. conference presentations, news posts, reports…)
- Which type of policing? (e.g. recent arrests, lack of seizures, future plans…)
- Policing operations that you were directly involved in or performed by others? If the former, do you reveal your involvement?
- How often?
- Who are the communications aimed at? (e.g. other policing agencies, wider public…)
- What is the purpose of these communications? (e.g. information sharing, progress reporting, awareness raising …)

Other

1) Any other comments or experiences that might prove useful for this study?
2) Do you know anyone else who might be able to help this investigation?

Appendix A.2: List of Europol's written online illegal drug trade policing publications (2007-2020) for content analysis

Organisation	Publication	Format
Europol (56)	Joint Report on a new psychoactive substance: 1-benzylpiperazine (BZP) (2007) [with EMCDDA]	Report
	Annual Report on the implementation of Council Decision 2005/387/JHA (2008) [with EMCDDA]	Report
	Annual Report on the implementation of Council Decision 2005/387/JHA (2009) [with EMCDDA]	Report
	Annual Report on the Implementation of Council Decision 2005/387/JHA (2010a) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: 4-methylmethcathinone (mephedrone) (2010b) [with EMCDDA]	Report
	Annual Report on the implementation of Council Decision 2005/387/JHA (2011) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: 4-methylamphetamine (2012a) [with EMCDDA]	Report
	New drugs in Europe - Annual Report on the implementation of Council Decision 2005/387/JHA (2012b) [with EMCDDA]	Report
	Annual Report on the implementation of Council Decision 2005/387/JHA (2013a) [with EMCDDA]	Report
	EU drug markets report - a strategic analysis (2013b) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: 5-(2-aminopropyl)indole (5-IT) (2013c) [with EMCDDA]	Report
	Annual Report on the implementation of Council Decision 2005/387/JHA (2014a) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: 1-cyclohexyl-4- (1,2-diphenylethyl)piperazine ('MT-45') (2014b) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: 4,4'-DMAR (4-methyl-5- (4-methylphenyl)-4,5-dihydrooxazol-2-amine) (2014c) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: 25I-NBOMe (4-iodo-2,5-dimethoxy-N-(2-methoxybenzyl)phenethylamine) (2014d) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: AH-7921 3,4-dichloro-N-([1-(dimethylamino)cyclohexyl] methyl)benzamide (2014e) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: MDPV (3,4-methylenedioxypyrovalerone) (2014f) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: methoxetamine (2-(3-methoxyphenyl)-2-(ethylamino) cyclohexanone) (2014g) [with EMCDDA]	Report
	EC3 first year report (2014a)	Report
	Europol Review - general report on Europol activities (2014b)	Report
	Global action against Dark Markets on Tor network (2014c)	News article
	Internet Organised Crime Threat Assessment (IOCTA) (2014d)	Report
	Annual Report on the implementation of Council Decision 2005/387/JHA (2015) [with EMCDDA]	Report
	Europol Review - general report on Europol activities (2015b)	Report

	Internet Organised Crime Threat Assessment (IOCTA) (2015c)	Report
	Annual Report on the implementation of Council Decision 2005/387/JHA (2016a) [with EMCDDA]	Report
	EU drug market markets report - in-depth analysis (2016b) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: methyl 2-[[1-(cyclohexylmethyl)indoP-3-carbonyl]amino]- 3,3-dimethylbutanoate (MDMB-CHMICA) (2016c) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: N-phenyl-N-[1-(2-phenylethyl)piperidin-4-yl] acetamide (acetylfentanyl) (2016d) [with EMCDDA]	Report
	Europol and EMCDDA: excellent cooperation to combat the illicit drug markets in the EU (2016a)	News article
	Internet Organised Crime Threat Assessment (IOCTA) (2016b)	Report
	Drugs and the darknet - perspectives for enforcement, research and policy (2017a) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: N-(1-phenethylpiperidin-4-yl)- N-phenylacrylamide (acryloylfentanyl) (2017b) [with EMCDDA]	Report
	Joint Report on a new psychoactive substance: N-phenyl-N-[1-(2-phenylethyl) piperidin-4-yl]-furan-2-carboxamide (furanylfentanyl) (2017c) [with EMCDDA]	Report
	Darknet dealer of drugs and arms arrested by Slovak authorities (2017a)	News article
	Drugs in Europe: a bold Police response (2017c)	News article
	Europol Review 2016-2017 (2017d)	Report
	Internet Organised Crime Threat Assessment (IOCTA) (2017e)	Report
	Massive blow to criminal dark web activities after globally coordinated (2017f)	News article
	Serious and Organised Crime Threat Assessment (SOCTA) (2017g)	Report
	Crime on the dark web: Police coordination is the only cure (2018a)	News article
	'Drugs in Europe: a bold Police response' second annual conference (2018b)	News article
	Internet Organised Crime Threat Assessment (IOCTA) (2018c)	Report
	EU drug markets report (2019) [with EMCDDA]	Report
	Common challenges in combatting cybercrime (2019) [with Eurojust]	Report
	Deepdotweb shut down: administrators suspected of receiving millions of kickbacks from illegal dark web proceeds (2019a)	News article
	Double blow to dark web marketplaces (2019b)	News article
	Europol's 20 most noteworthy operations (2019c)	Webpage
	Global Police action against vendors and buyers on the dark web (2019d)	News article
	Illicit drugs in the EU: the situation is expanding in scale and complexity (2019e)	News article
	International drug trafficking network disrupted (2019f)	News article
	Internet Organised Crime Threat Assessment (IOCTA) (2019g)	Report
	xDedic marketplace shut down in international operation (2019h)	News article
	International sting against Dark Web vendors leads to 179 arrests (2020d)	Report
	Internet Organised Crime Threat Assessment (IOCTA) (2020e)	News article
	Polish police take criminal gang selling fake impotence treatments off the market (2020f)	News article

Appendix A.3: List of UNODC's written online illegal drug trade policing publications (2012-2020) for content analysis

Organisation	Publication	Format
UNODC (17)	World Drug Report (2012b)	Report
	World Drug Report (2014)	Report
	World Drug Report (2015)	Report
	World Drug Report (2016a)	Report
	World Drug Report 1 – Executive summary, conclusions and policy implications (2017a)	Report
	World Drug Report 2 – Global overview of drug demand and supply: latest trends, cross-cutting issues (2017b)	Report
	World Drug Report 4 – Market analysis of synthetic drugs: amphetamine-type stimulants, new psychoactive substances (2017c)	Report
	World Drug Report 1 - Executive summary, conclusions and policy implications (2018b)	Report
	World Drug Report 2 - Global overview of drug demand and supply: latest trends, cross-cutting issues (2018c)	Report
	World Drug Report 3 – Analysis of drug markets: opiates, cocaine, cannabis, synthetic drugs (2018d)	Report
	World Drug Report 4 - Drugs and age: drugs and associated issues among young people and older people (2018e)	Report
	World Drug Report 5 – Women and drugs: drug use, drug supply and their consequences (2018f)	Report
	World Drug Report 1 - Executive summary, conclusions and policy implications (2019a)	Report
	World Drug Report 2 - Global overview of drug demand and supply (2019b)	Report
	World Drug Report 4 - Stimulants (2019c)	Report
	World Drug Report 1 – Executive summary, impact of covid-19, policy implications (2020c)	Report
	World Drug Report 4 – Cross-cutting issues: evolving trends and new challenges (2020d)	Report

Appendix A.4: List of WCO's written online illegal drug trade policing publications (2009-2020) for content analysis

Organisation	Publication	Format
WCO (17)	International operation combats the online supply of counterfeit and illegal medicines (2009)	News article
	Strong public safety focus of global operation targeting counterfeit and illegal medicines traded online (2010a)	News article
	WCO News (2010b)	Magazine
	Global operation strikes at online supply of illegal and counterfeit medicines worldwide (2011)	News article
	Annual report 2011-2012 (2012a)	Report
	Tackling organised crime networks behind global crackdown on illicit online pharmacies (2012b)	News article
	WCO News (2012c)	Magazine
	Annual report 2012-2013 (2013a)	Report
	International operation targets online sale of illicit medicines (2013b)	News article
	Illicit trade report (2014a)	Report
	Thousands of illicit online pharmacies shut down in global operation targeting fake medicines (2014b)	News article
	Millions USD worth illicit medicines seized in global operation (2015a)	News article
	WCO News (2015b)	Magazine
	WCO News (2016b)	Magazine
	WCO participates in Operation Pangea IX against fake and illicit medicines (2016c)	News article
	Illicit trade report (2018)	Report
	COVID-19 Urgent Notice: counterfeit medical supplies and introduction of export controls on personal protective equipment (2020a)	News article

Appendix A.5: List of written online illegal wildlife trade policing publications analysed for each Police agency (2011-2020)

Organisation	Publication	Format
Europol (4)	OC-SCAN Policy Brief - Trafficking in Endangered Species by Organised Crime Groups (2011b)	Policy Brief
	EnviCrimeNet Intelligence Project on Environmental Crime – Report on environmental crime in Europe (2015a)	Report
	28 bird traffickers netting €1 million per year arrested in Spain (Europol, 2020a)	News article
	Spain and Portugal take illegal ivory off the black market (2020g)	News article
UNODC (4)	Wildlife and forest crime analytic toolkit (2012a)	Toolkit
	World wildlife crime report – trafficking in protected species (2016b)	Report
	Guide on drafting legislation to combat wildlife crime (2018a)	Guide
	World wildlife crime report – trafficking in protected species (2020e)	Report
WCO (2)	French Customs seizes hundreds of archaeological objects and endangered wildlife products (2016a)	News article
	Wildlife trafficking: organised crime hit hard by joint WCO-INTERPOL global enforcement operation (2019)	News article

Appendix A.6: Coding scheme

The parts of the overall coding scheme relevant for the above analysis are presented below.

Policing of online trade	**Type of policing mentioned**	**Status of policing**	**Policing with others**	**Role in policing**
0. Not mentioned	0. None	0. Not mentioned	0. Not mentioned	0. None
1. Named in passing	1. General policing	1. Successful	1. Yes	1. Command post
2. Mentioned or defined briefly	2. Market takedown	2. Unsuccessful	2. No	2. Coordination
3. Covered in detail	3. Several markets taken down	3. In progress		3. Power of arrest and takedown
	4. Individual arrest	4. Hypothetical		4. Information exchange
	5. Several arrests	5. Lack of		5. Operational expertise
	6. Network dismantled	6. Future		6. Analytical support
	7. Investigation	7. Theoretical		7. Forensic support
	8. Seizure(s)			8. Intelligence provision, incl evidence
	9. Prosecution and conviction			9. Awareness raising
	10. Content removal			10. Software provision
	11. User blocking			
	12. Exit scam(s)			
	13. Market closure(s)			
	14. Distributed Denial of Service attack(s)			
	15. Controls and sanctions, incl policies			
	16. Users stop trading			
	17. Monitoring and detection, incl by users			
	18. Education and raising awareness			
	19. Forgeries			
	20. Scams			
	21. Product ban			
	22. Deterrence and prevention			
	23. Law			
	24. Identification of suspects			
	25. Honeypot			
	26. Market penetration			

Appendix B.1: Legal online platforms interview topics

About you

1) Why did you choose to work for your organisation?
2) What does your current position entail?
3) Do you get to experience the policing of online illegal drug/wildlife trade on your platform as part of this position?
4) How long have you been working for your organisation?

Trade policies and Content monitoring

1) Does your platform show specific trade policies to users?
2) If so, how were these policies put together? Did you collaborate with other legal platforms or organisations to devise them?
3) Are warnings about punishments available to users if breaking these rules?
4) How do you monitor for illegal content on your platform?
5) What do you consider your organisation's best strategic decision so far in that respect?

Policing of online illegal drug/wildlife trade

1) What policing activities does your platform take part in? (e.g. content removal, account blocking, law enforcement reporting…)
2) What have users' responses been to your current policing approaches?
3) Do you collaborate with any of the below for your work? If so which ones, for what purpose(s), how (e.g. meetings, emails, calls, trainings…), and how often?

- Police agencies whether regional or international
- Industry (e.g. private organisations, other legal platforms …)
- Non-profits
- Inter-Governmental Organisations
- Policymakers
- Schools and Universities

4) How do the different entities' skills complement each other?

5) How often do you organise / attend inter-sector meetings about the policing of online illegal drug/wildlife trade? What are the other sectors represented? What is the main aim of these meetings?

Communication about online illegal drug/wildlife trade policing

Do you ever publicly communicate, verbally or in writing, about online illegal drug/wildlife trade policing?

- What types of communications? (e.g. news posts, reports…)
- Which type of policing? (e.g. content removal, account blocking, future plans…)
- Policing operations that you were directly involved in or performed by others? If the former do you reveal your involvement?
- How often?
- Who are the communications aimed at? (e.g. other policing actors, wider public…)
- What is the purpose of these communications? (e.g. information sharing, progress reporting, awareness raising …)

Other

1) Any other comments or experiences that might prove useful for this study?
2) Do you know anyone else who might be able to help this investigation?

Appendix B.2: List of online illegal drug trade policies published by each online platform for content analysis

Organisation	Publication	Format
eBay (3)	Illegal drugs and drug paraphernalia policy (2020b)	Policy
	Prescription and over-the-counter drug policy (2020d)	Policy
	Report an item or listing (2020e)	Policy
Etsy (1)	Prohibited items policy (2020)	Policy
Facebook (6)	Facebook, Instagram announce new educational enforcement measures for commercial activity (2014)	Blog post
	How we enforce against illicit drug sales (2018a)	Blog post
	Supporting our community in the face of the opioid epidemic (2018b)	Blog post
	Community standards enforcement report, November 2019 edition (2019a)	Report
	An update on how we are doing at enforcing our community standards (2019b)	Report
	Regulated goods (2020)	Policy
Freeads (3)	Why is my ad not live yet? (2019c)	Blog post
	How to report an advert (2020a)	Policy
	Posting rules (2020c)	Policy
Gumtree (2)	Reporting an ad (2020d)	Policy
	What's not allowed on Gumtree? (2020e)	Policy
Instagram (1)	Community guidelines (2020)	Policy
Twitter (1)	Illegal or certain regulated goods or services (2019)	Policy
WeChat (1)	Acceptable use policy (2015)	Policy
WhatsApp (1)	Commerce Policy (2019)	Policy

Appendix B.3: List of online illegal wildlife trade policies published by each online platform for content analysis

Organisation	Publication	Format
eBay (14)	eBay to institute global ban on ivory sales (2008a)	Blog post
	IFAW applauds eBay for global ivory ban: an interview with Barbara Cartwright, IFAW campaign manager (2008b)	Blog post
	Global impact 2016 report (2016a)	Report
	On Earth Day and every day, eBay is working to end wildlife trafficking (2016b)	Blog post
	Working together to end wildlife trafficking (2016c)	Blog post
	eBay impact 2017 progress update (2017a)	Report
	Taking steps to combat illegal wildlife trafficking (2017b)	Blog post
	eBay Impact 2018 progress update (2018a)	Report
	Supporting world elephant day (2018b)	Blog post
	eBay celebrates global tiger day with World Wildlife Fund (2019a)	Blog post
	eBay partners with the International Fund for Animal Welfare in honor of its 10-year anniversary on global ban of ivory sales (2019b)	Blog post
	Animal products policy (2020a)	Policy
	Live animals policy (2020c)	Policy
	Report an item or listing (2020e)	Policy
Etsy (2)	Company news - Working together to end illegal wildlife trafficking (2016)	Blog post
	Prohibited items policy (2020)	Policy
Facebook (4)	Facebook, Instagram announce new educational enforcement measures for commercial activity (2014)	Blog post
	Community standards enforcement report, November 2019 edition (2019a)	Report
	An update on how we are doing at enforcing our community standards (2019b)	Report
	Regulated goods (2020)	Policy
Freeads (4)	Why is my ad not live yet? (2019c)	Blog post
	How to report an advert (2020a)	Policy
	Pet advert posting rules (2020b)	Policy
	Posting rules (2020c)	Policy
Gumtree (5)	Animals we do not allow (2020a)	Policy
	Pet policies (2020b)	Policy
	Protecting pets by making our pets category harder to use (2020c)	Blog post
	Reporting an ad (2020d)	Policy
	What's not allowed on Gumtree? (2020e)	Policy
Instagram (1)	Community guidelines (2020)	Policy
Pets4Homes(1)	Terms and Conditions (2020)	Policy
Preloved (5)	Preloved listing guidelines (2015a)	Blog post
	Press release – Preloved bans sale of ivory (2015b)	Policy
	Why Preloved does not allow the sale of ivory (2015d)	Blog post
	CoP17: CITES updates for endangered species (2017)	Blog post
	Selling endangered species (2020)	Policy
Twitter (1)	Illegal or certain regulated goods or services (2019)	Policy
WeChat (1)	Acceptable use policy (2015)	Policy
WhatsApp (1)	Commerce Policy (2019)	Policy

Appendix B.4: Content analysis

Unlike other chapters about the Police and private organisations and individuals, legal online platform policies were not analysed following a coding scheme. Instead, keywords were counted and reported across platforms in order to signal the breadth of terms used in these policies and the discrepancies present between marketplaces. Such an analysis would therefore not have been possible if these keywords had been amalgamated in similar codes, as was the case for the other documents analysed in this thesis. Indeed, these codes need to be designed prior to the analysis and broad enough to relate to the various documents under investigation. In the case of these trade policies, the breadth of vocabulary used to define the terms of interest needed to be preserved, and these could not be designed in advance.

All the relevant information about the keywords counted and analysed can be found in the Methods and Legal online platforms chapters.

Appendix C.1: Organisations and Individuals interview topics

About you

1) Why did you choose to work for your organisation?
2) What does your current position entail?
3) Do you get to experience the policing of online illegal drug/wildlife trade as part of this position?
4) How long have you been working for your organisation?

Operational and strategic evolution

1) How long has your organisation been involved in the policing of online illegal drug/wildlife trade?
2) What specific work has your organisation been involved in? (e.g. regulation, trade monitoring, arrests, seizures, platform content removal…)
3) During your time there, what major operational and strategic changes occurred as to your organisation's approach to the policing of online illegal drug/wildlife trade?
4) What do you consider your organisation's best strategic decision so far in that respect?

Policing of online illegal trade

1) Do you have thoughts or ideas about the best ways to reduce online illegal drug/wildlife trade?
2) Do you collaborate with any of the below for your work? If so which ones, for what purpose(s), how (e.g. meetings, emails, calls, trainings…), and how often?

- Police agencies whether regional or international
- Industry (e.g. private organisations, legal platforms …)
- Non-profits
- Inter-Governmental Organisations
- Policymakers
- Schools and Universities

3) How do the different entities' skills complement each other?

4) How often do you organise / attend inter-sector meetings about the policing of online illegal drug/wildlife trade? What are the other sectors represented? What is the main aim of these meetings?

Communication about online illegal trade policing

Do you ever publicly communicate, verbally or in writing, about online illegal drug/wildlife trade policing?

- What types of communications? (e.g. conference presentations, news posts, reports…)
- Which type of policing? (e.g. recent arrests, lack of seizures, future plans…)
- Policing operations that you were directly involved in or performed by others? If the former, do you reveal your involvement?
- How often?
- Who are the communications aimed at? (e.g. other policing actors, wider public…)
- What is the purpose of these communications? (e.g. information sharing, progress reporting, awareness raising …)

Other

1) Any other comments or experiences that might prove useful for this study?
2) Do you know anyone else who might be able to help this investigation?

Appendix C.2: List of written online illegal drug trade policing publications analysed for each private organisation

Organisation	Publication	Format
CSIP (17)	Mastercard works with Interpol to keep consumers safe (2012)	Blog post
	Black market site "Silk Road" re-emerges (2013a)	Blog post
	Companies join forces to protect consumers from the prevalent threat of illegal online pharmacies (2013b)	Blog post
	Google taking steps to curtail counterfeit pharmacies (2013c)	Blog post
	Major underground online drug market shut down (2013d)	Blog post
	CSIP member Microsoft opens center to fight cybercrime (CSIP, 2014a)	Blog post
	CSIP participates in global Law Enforcement operation targeting fake medicines (CSIP, 2014b)	Blog post
	CSIP partners help shut down rogue online pharmacies (CSIP, 2014c)	Blog post
	Operation Pangea VII targets social media (CSIP, 2014d)	Blog post
	Rogue online drug marketplaces pose dangers for consumers (CSIP, 2014e)	Blog post
	Operation Pangea VIII targets illicit websites and medical devices (CSIP, 2016a)	Blog post
	Our members: continuing the fight against rogue online pharmacies (CSIP, 2016b)	Blog post
	Our members: fighting against rogue online pharmacies (CSIP, 2016c)	Blog post
	Operation Pangea X successfully targets websites selling fake opioids and other dangerous drugs (CSIP, 2017)	Blog post
	Facebook changes ad policies for addiction treatment centers to protect consumers (CSIP, 2018)	Blog post
	CSIP urges consumers to report fraudulent medications that claim to treat or prevent COVID-19 (CSIP, 2020a)	Blog post
	Tracking illegal opioid sales using social media data (CSIP, 2020b)	Blog post
Cyjax (5)	The Darknet after AlphaBay and Hansa (2017)	Blog post
	Darknet Markets: no honour among thieves (2018a)	Blog post
	Darknet Review - April (2018b)	Blog post
	Darknet Quarterly Review - Q2 July (Cyjax, 2020c)	Blog post
	Darknet Quarterly Review - March (2020d)	Blog post
Flashpoint (8)	Highlights and trends in the Deep Dark Web (2016)	Report
	Fentanyl sales in the Deep and Dark Web (2017a)	Blog post
	US DOJ announces takedowns of AlphaBay and Hansa underground markets (2017b)	Blog post
	Inside the underground of trade prescription drugs (2018a)	Blog post
	Wait continues for AlphaBay's successor (2018b)	Blog post
	Expansive access to illicit activity on chat services platforms lowers risk (2019a)	Blog post
	Looking at Darknet marketplaces through a Brazilian lens (2019b)	Blog post
	Popular Narcotics across Illicit Online Communities and Marketplaces (2020)	Blog post

Appendix C.3: List of written online illegal wildlife trade policing publications analysed for each private organisation

Organisation	Publication	Format
IFAW (18)	Elephants on the high street (2004)	Report
	Caught in the web (2005)	Report
	Bidding for extinction (2007)	Report
	Global security implications (2008a)	Report
	Killing with keystrokes (2008b)	Report
	Killing with keystrokes 2.0 (2011)	Report
	Making a killing (2012)	Report
	Global security implications (2013)	Report
	Bidding against survival (2014a)	Report
	Click to delete (2014b)	Report
	Elephant vs Mouse (2014c)	Report
	Wanted dead or alive (2014d)	Report
	Ivory seizures (2017a)	Report
	Out of Africa (2017b)	Report
	Wildlife friendly online policies (2017) [with WWF and TRAFFIC]	Plan
	Disrupt wildlife cybercrime (2018a)	Report
	Global wildlife cybercrime action plan (2018b)	Plan
	Offline and in the wild: a progress report of the Coalition to End Wildlife Trafficking Online (2020) [with WWF and TRAFFIC]	Report
WJC (10)	Governments urged to support Vietnam (2016a)	Blog post
	Independent panel recommendations (2016b)	Blog post
	Operation Ambush (2016c)	Report
	Vietnam recommendations from around the world (2016d)	Blog post
	Black Business (2017a)	Report
	Operation Phoenix (2017b)	Report
	Operation dragon (2018a)	Report
	Raw rhino horn (2018b)	Report
	Freshwater turtles (2018c)	Report
	Scaling up (2020c)	Report

Appendix C.4: Coding scheme

The parts of the overall coding scheme relevant for the above analysis are presented below.

Policing of online trade	**Type of policing mentioned**	**Status of policing**	**Policing with others**	**Role in policing**
0. Not mentioned	0. None	0. Not mentioned	0. Not mentioned	0. None
1. Named in passing	1. General policing	1. Successful	1. Yes	1. Command post
2. Mentioned or defined briefly	2. Market takedown	2. Unsuccessful	2. No	2. Coordination
3. Covered in detail	3. Several markets taken down	3. In progress		3. Power of arrest and takedown
	4. Individual arrest	4. Hypothetical		4. Information exchange
	5. Several arrests	5. Lack of		5. Operational expertise
	6. Network dismantled	6. Future		6. Analytical support
	7. Investigation	7. Theoretical		7. Forensic support
	8. Seizure(s)			8. Intelligence provision, incl evidence
	9. Prosecution and conviction			9. Awareness raising
	10. Content removal			10. Software provision
	11. User blocking			
	12. Exit scam(s)			
	13. Market closure(s)			
	14. Distributed Denial of Service attack(s)			
	15. Controls and sanctions, incl policies			
	16. Users stop trading			
	17. Monitoring and detection, incl by users			
	18. Education and raising awareness			
	19. Forgeries			
	20. Scams			
	21. Product ban			
	22. Deterrence and prevention			
	23. Law			
	24. Identification of suspects			
	25. Honeypot			
	26. Market penetration			

Appendix D.1 – Experiment instructions

The experiment instructions are presented below from the CONTROL, SLANDER treatment 1, and SYBIL treatment 2.

All sections of the experiment remain the same and, unless indicated otherwise, apply to all treatments. Underlined sections apply only to SLANDER treatment 1 and italicised ones only to SYBIL treatment 2, as their designs included additional steps.

Participants could only see instructions for their own treatment session and were not informed which treatment they were participating in.

Experiment instructions were provided in paper and digital form to all participants upon sitting at their workstations and read out loud by the researcher before the experiment started.

Welcome to this experiment and thank you for participating. Please read the following instructions carefully.

This is an experiment in decision-making in situations of uncertainty. It consists of four tasks, each of which will be explained as that part of the experiment begins. The amount of money you earn from this experiment may depend on the decisions you make, the decisions others make, and luck.

During the experiment, your earnings are given in tokens. At the end of the experiment you will be paid in CASH based on the following exchange rate:

25 tokens = 1 GBP

Other participants will not be able to see how much you have earned.

This experiment will last approximately 90mins. Please do not talk or communicate with other participants during the experiment or look at other participants' computer screens. Please turn off your mobile phones to avoid any distractions.

If you have any questions, please raise your hand and someone will come to help you.

First task

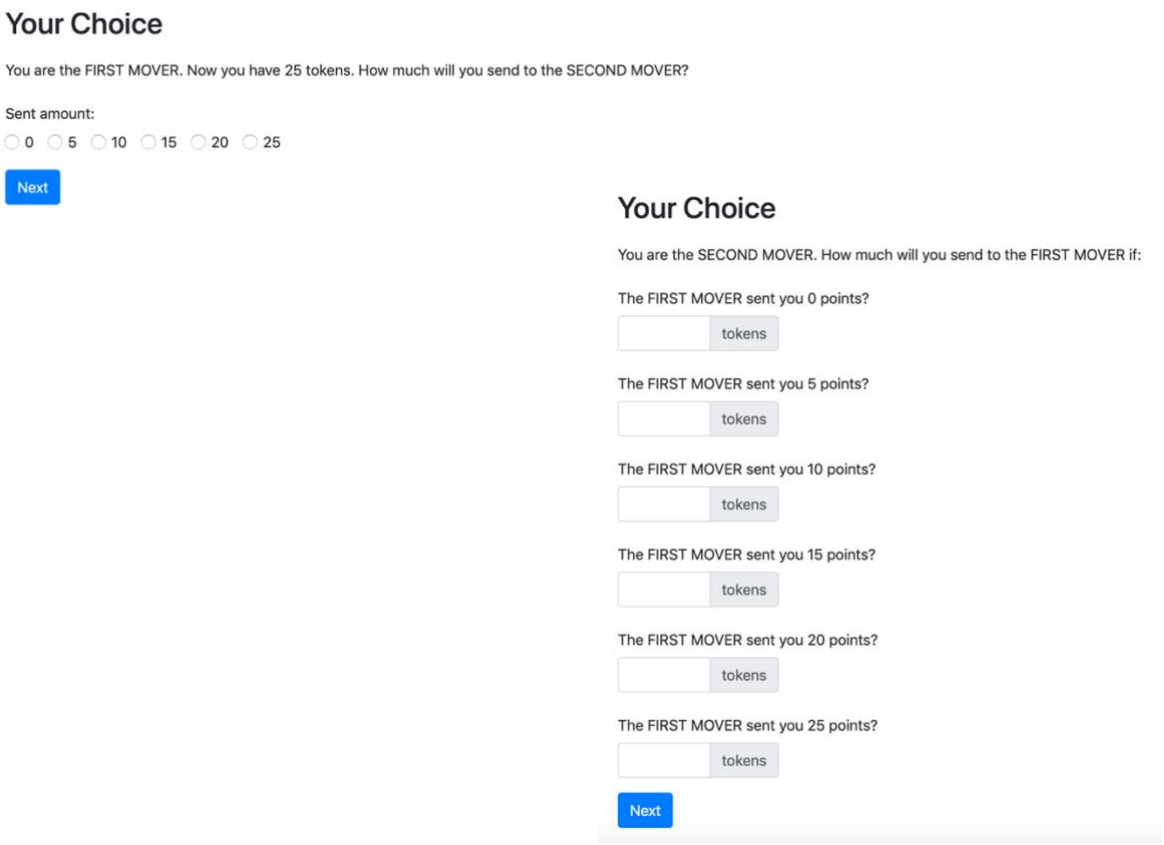
In this task you are randomly paired up with two other participants one after the other.

In each pair, one of you is the FIRST MOVER and the other the SECOND MOVER. Each participant begins with **25 tokens**.

FIRST MOVERS choose to send none, some, or all of their 25 tokens to SECOND MOVERS. Once they have chosen the amount to send, SECOND MOVERS receive three times the amount sent to them. SECOND MOVERS then decide how many of their tokens to now send back to FIRST MOVERS, none, some, or all.

Neither the experimenters nor the participants know how much the FIRST MOVERS will send. As a result, SECOND MOVERS choose how much they would like to return to FIRST MOVERS for each possible amount they could have been sent.

Both FIRST and SECOND movers can only send multiples of five tokens (e.g. 0, 5, 10, 15, 20, 25) to one another.



For example:

- FIRST MOVER and SECOND MOVER both start with 25 tokens;
- FIRST MOVER sends 10 tokens to SECOND MOVER;
- SECOND MOVER receives 30 tokens and now has 55 tokens;
- SECOND MOVER sends 15 tokens back to FIRST MOVER;
- FIRST MOVER receives 15 tokens;
- FIRST MOVER now has a total payoff of: 25 - 10 + 15 = 30 tokens and SECOND MOVER of: 25 + 30 - 15 = 40 tokens.

Or:

- FIRST MOVER and SECOND MOVER both start with 25 tokens;
- FIRST MOVER sends 20 tokens to SECOND MOVER;
- SECOND MOVER receives 60 tokens and now has 85 tokens;
- SECOND MOVER sends 10 tokens back to FIRST MOVER;
- FIRST MOVER receives 10 tokens;
- FIRST MOVER now has a total payoff of: 25 - 20 + 10 = 15 tokens and SECOND MOVER of: 25 + 60 - 10 = 75 tokens.

You are either a FIRST MOVER or SECOND MOVER in each pair. Which mover you are in the first pair is decided at random. In the second pair you are the other mover.

You will be remunerated for one of these two decisions, chosen at random, either the one that you made as a FIRST MOVER or as a SECOND MOVER. Your payoff will depend on both the decision you made and the decision your partner made. You will not see the results of the decisions (and the corresponding payment) until the end of the experiment.

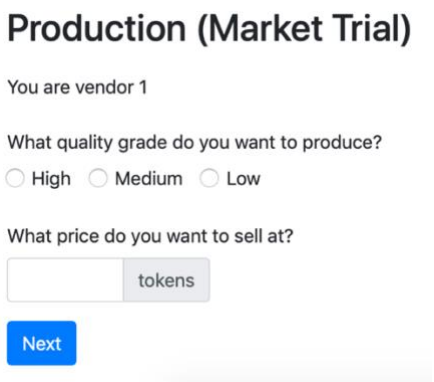
You will initially perform a trial round before the 'real' task begins, which will not impact your earnings.

Second task

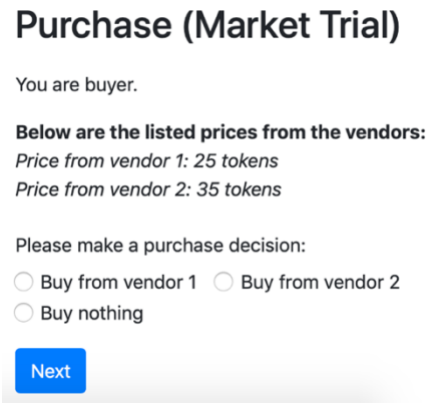
In the second task, there are 30 rounds. You are either a BUYER or a VENDOR for the entirety of this task. In each round, you are randomly assigned to a group with two other participants. In each round, one group member is a BUYER and the other two are VENDORS.

At the beginning of each round, all VENDORS and BUYERS receive **50 tokens**.

VENDORS begin by privately choosing a price (between 0 and 50 tokens) and a quality grade for their products - high, medium, or low; a higher grade costs more to produce for VENDORS and is worth more to BUYERS.

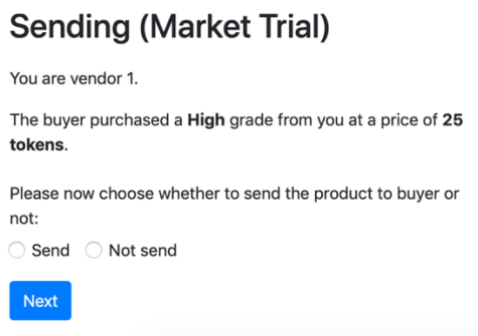


BUYERS then have a chance to purchase from either of the VENDORS in their group at the prices listed observing **price alone**. Otherwise, they can choose not to buy from either VENDOR.



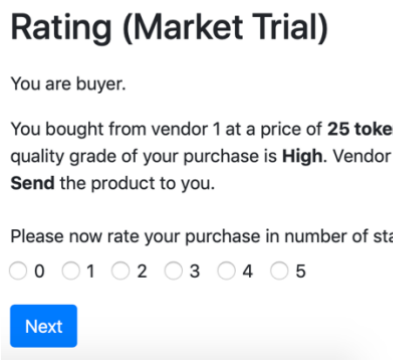
After each sale, VENDORS are given the option not to 'send' the products to BUYERS, meaning they would receive money from the sale without paying for its production.

*In SYBIL (treatment 2): After each sale, VENDORS are given the option not to 'send' the products to BUYERS, meaning they would be receiving money from the sale without paying for its production. However, if a VENDOR chooses to 'send' the product, there is a 15% chance for each VENDOR during each round that this decision will be '**compromised'** and instead replaced by a decision 'not to send'. This does not affect the VENDOR's payoffs and they are charged for the production costs as they would have been if the product had been 'sent'. Decisions 'not to send' always go through 'uncompromised'. Participants are not informed which 'sending' decisions have been 'compromised'.*



BUYERS are then asked to rate the quality of the product they just acquired, based on its price, quality, and whether they received it or not, on a **scale of 0 to 5**. These ratings build on each other throughout rounds and the average of all ratings received by VENDORS is displayed for the duration of the Task.

In SLANDER (treatment 1): BUYERS are then asked to rate the quality of the product they just acquired, based on its price, quality, and whether they have received them or not, on a **scale of 0 to 5**. These ratings build on each other throughout rounds and the average of all ratings received by VENDORS is displayed for the duration of the Task. However, there is a 15% chance for each BUYER during each round that these ratings will be '**compromised',** meaning they are discarded and replaced by a randomly chosen different rating. Every other rating than the one that was initially given by the BUYER has an equal chance to be chosen to replace it. Participants are not informed which ratings have been compromised and the compromised ratings are included in the VENDORS' averaged ratings.



BUYERS can buy up to 1 unit of the commodity during a round. VENDORS can produce up to 1 unit in a round.

VENDORS in each group who are not chosen by buyers end the round with 0 tokens.

BUYERS who choose not to buy from either vendor end the round with 0 tokens.

For example (CONTROL):

- Round 4:
- VENDOR 1 (4.7/5 stars) chooses a price of 25 tokens and Medium quality for its product and VENDOR 2 (4.5/5 stars) chooses a price of 25 tokens and Low quality;
- BUYER can only see the prices on offer and chooses VENDOR 1's offer;
- VENDOR 1 then chooses to send the product to BUYER;
- BUYER rates the purchase 4 out of 5 stars.

Or:

- Round 17:
- VENDOR 1 (3/5 stars) chooses a price of 40 tokens and Medium quality for its product and VENDOR 2 (4.1/5 stars) chooses a price of 30 tokens and Low quality;
- BUYER can only see the prices on offer and chooses VENDOR 2's offer;
- VENDOR 2 then chooses not to send the product to BUYER;
- BUYER rates the purchase 0 out of 5 stars.

For example (SLANDER treatment 1):

- Round 4:
- VENDOR 1 (4.7/5 stars) chooses a price of 25 tokens and Medium quality for its product and VENDOR 2 (4.5/5 stars) chooses a price of 25 tokens and Low quality;
- BUYER can only see the prices on offer and chooses VENDOR 1's offer;
- VENDOR 1 then chooses to send the product to BUYER;
- BUYER rates the purchase 4 out of 5 stars;
- <u>The rating is not compromised and stays 4 out of 5 stars.</u>

Or:

- Round 17:
- VENDOR 1 (3/5 stars) chooses a price of 40 tokens and Medium quality for its product and VENDOR 2 (4.1/5 stars) chooses a price of 30 tokens and Low quality;
- BUYER can only see the prices on offer and chooses VENDOR 2's offer;
- VENDOR 2 then chooses not to send the product to BUYER;
- BUYER rates the purchase 0 out of 5 stars;
- <u>The rating is compromised and becomes 3 out of 5 stars.</u>

For example (SYBIL treatment 2):

- Round 4:
- VENDOR 1 (4.7/5 stars) chooses a price of 25 tokens and Medium quality for its product and VENDOR 2 (4.5/5 stars) chooses a price of 25 tokens and Low quality;
- BUYER can only see the prices on offer and chooses VENDOR 1's offer;
- VENDOR 1 then chooses to send the product to BUYER;
- *The sending decision is compromised to 'not to send';*
- BUYER rates the purchase 0 out of 5 stars.

Or:

- Round 17:
- VENDOR 1 (3/5 stars) chooses a price of 40 tokens and Medium quality for its product and VENDOR 2 (4.1/5 stars) chooses a price of 30 tokens and Low quality;
- BUYER can only see the prices on offer and chooses VENDOR 2's offer;
- VENDOR 2 then chooses not to send the product to BUYER;
- BUYER rates the purchase 0 out of 5 stars.

You will be remunerated for 5 of the 30 rounds in this Task, all chosen at random.

You will initially perform a trial round before the 'real' 30 rounds begin, which will not impact your earnings.

Third task

In this task you are randomly paired with two other participants in the session and perform two decisions, one as FIRST MOVER and the other as SECOND MOVER, each in a different pair, like in the First task. You will be remunerated for one of these two decisions chosen at random, either the one that you made as a FIRST MOVER or as a SECOND MOVER.

Each participant begins with **25 tokens**.

FIRST MOVERS choose to send none, some, or all of their 25 tokens to SECOND MOVERS. Once they have chosen the amount to send, SECOND MOVERS receive three times the amount sent to them. SECOND MOVERS then decide how many of their tokens to send back to FIRST MOVERS, none, some, or all.

Neither the experimenters nor the subjects know how much the FIRST MOVER will send. As a result, SECOND MOVERS choose how much they would like to return for each possible amount they could be sent.

Both FIRST and SECOND movers can only send multiples of five tokens (e.g. 0, 5, 10, 15, 20, 25) to one another.

Fourth task

You are finally asked to complete several survey questions following this study. Some questions are demographic (eg age, gender, occupation, degree), while others are about your strategy in the experiment and perception of other players' strategies. Your answers will not be matched with your name and will be kept anonymous, so please answer honestly. This survey takes approximately 5 minutes to complete. Please take your time to answer all of the questions while we prepare your individual cash payment.

You will then find out the outcome and your total payoffs from the experiment. All final payments will be rounded up to the nearest Pound.

Please stay seated until the experimenter calls you to receive your payment.

Thank you for your participation!

Appendix D.2 – Vendor and buyer payoffs

Payoff information was provided on a separate sheet based on the participants' assigned roles. Each participant only received one bit of information, either that of a vendor or a buyer.

In this Task you are a **VENDOR**.

The table below shows production costs for different grades, buyers cannot see this information:

Grade	High	Medium	Low
Production cost to vendors	30	20	10

The period payoff for VENDORS is: **50 tokens + vendor's price – cost of the grade produced (if sent)**

VENDORS in each group who are not chosen by buyers end the round with 0 tokens.

In this Task you are a **BUYER**.

The table below shows values for different grades, vendors cannot see this information:

Grade	High	Medium	Low
Value to buyer	45	30	15

The period payoff for BUYERS is: **50 tokens + value of the grade purchased (if sent) – vendor's price**

BUYERS who choose not to buy from either vendor end the round with 0 tokens.

Appendix D.3 – Market for lemons results

Results of the "market for lemons" experimental sessions are presented below, including prices offered and prices purchased. In the following tables, prices purchased are presented in bold. The number of prices presented varies between sessions because the CONTROL sessions had 6 fewer participants than SLANDER and SYBIL sessions. Additionally, the number of purchase prices emboldened also varies between rounds, as some participants sometimes chose not to buy. The number of buyers (and with it the maximum number of purchase prices per round) was 14 in the Control and 16 in the slander and Sybil treatments.

The number of products offered in each quality grade is also presented. It should be noted that the total number of products per session varies between the CONTROL and SLANDER and SYBIL treatments, as there were 4 fewer vendors to offer their products in the CONTROL than in the other sessions.

Control sessions – prices offered and purchase prices for every round

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
10	5	5	**0**	0	0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
10	**10**	**10**	**0**	**5**	**5**	0	0	**5**	5	**5**	**0**	**0**	0	**0**	**0**	**0**	5	**0**	**5**	**0**	0	0	**0**	**0**	**0**	**0**	**0**	**0**	**0**
10	10	**10**	**5**	**15**	**10**	5	**5**	**5**	5	5	**5**	5	**5**	0	0	0	**5**	**5**	**5**	**5**	**5**	**5**	**5**	**5**	0	**0**	0	**0**	**0**
15	15	10	**5**	**15**	10	**10**	**5**	**10**	5	10	**5**	10	**5**	**10**	**5**	**5**	**5**	5	5	**10**	**5**	**5**	**5**	5	**5**	0	0	0	0
15	15	10	**15**	**20**	**15**	10	10	**15**	10	**15**	**10**	**15**	5	**10**	**10**	**5**	**5**	**10**	**10**	**10**	5	5	**5**	5	5	**5**	**5**	**5**	**5**
15	**20**	**15**	**15**	**20**	**15**	**15**	**15**	15	**15**	**15**	10	**15**	10	10	10	**10**	**10**	**10**	10	10	5	10	10	5	5	**5**	**5**	**5**	**5**
20	**20**	**15**	**20**	**20**	**15**	**15**	**15**	15	**15**	**15**	**15**	**15**	10	10	10	**10**	10	**10**	10	10	10	10	10	**10**	**10**	**10**	**5**	**10**	**5**
20	**20**	**15**	**20**	**20**	15	15	**15**	20	**20**	15	15	**15**	**15**	10	10	10	**15**	**15**	**15**	**15**	**15**	**15**	10	**10**	**10**	**10**	5	**10**	5
20	**20**	**15**	**20**	20	**20**	**20**	15	20	**20**	**20**	15	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	15	**15**	**15**	**15**	10	**10**	10	**10**	10	**10**
20	**20**	15	20	20	**20**	20	**20**	20	**20**	**20**	15	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	15	15	**15**	**15**	10	10	10	10	10	10
20	**25**	15	20	20	**20**	**25**	20	20	**20**	20	15	**20**	**15**	**15**	15	**15**	**15**	15	15	15	15	15	**15**	**15**	15	15	10	**15**	**15**
25	**25**	15	20	20	20	**25**	**25**	**25**	20	20	**20**	20	15	**15**	15	**15**	**15**	15	15	**20**	20	15	15	15	**20**	20	**15**	20	**15**
25	**25**	**20**	20	**25**	20	**25**	**25**	25	20	20	**20**	20	**20**	**15**	**20**	15	15	20	15	**20**	20	**20**	**25**	15	20	**25**	15	**25**	15
25	**25**	**20**	20	**25**	20	**25**	**25**	25	**25**	**25**	20	20	20	15	**20**	15	15	**25**	**20**	20	20	**25**	**25**	15	**25**	**25**	**20**	**25**	15
25	**25**	**20**	**25**	25	**25**	**25**	**25**	25	**25**	25	20	20	20	**20**	**25**	15	15	**25**	**20**	20	**25**	25	25	**20**	**25**	**25**	20	**25**	15
30	**25**	**25**	**25**	25	**25**	**25**	25	25	25	25	**25**	**25**	**25**	20	**25**	20	20	25	**20**	**25**	**25**	25	25	**25**	**25**	**25**	**25**	25	**20**
30	25	25	25	**30**	25	25	25	25	**30**	25	**25**	25	**25**	**25**	**25**	20	20	25	20	25	**25**	25	25	**25**	**25**	**25**	**25**	25	**20**
30	25	25	25	**30**	25	25	**30**	**30**	**30**	**30**	25	25	25	25	25	**25**	20	25	20	25	**25**	25	25	**25**	25	**30**	25	25	20
30	25	25	25	30	**30**	25	30	**30**	30	**30**	25	**30**	25	25	25	**25**	**25**	25	**25**	**30**	**25**	**30**	**30**	25	25	**30**	25	25	20
30	**30**	25	25	30	**30**	**30**	30	**30**	30	**30**	**30**	**30**	**30**	25	25	25	25	**30**	25	**30**	25	**30**	**30**	**30**	25	30	25	25	**25**
30	30	**30**	**30**	**35**	30	**30**	30	30	30	30	**30**	30	**30**	25	**30**	**30**	**30**	**30**	25	**30**	**30**	**30**	**30**	**30**	**30**	30	**30**	25	**25**
30	30	30	30	**35**	30	30	**35**	30	30	30	**30**	**35**	**30**	**30**	30	30	30	30	25	**30**	**30**	**30**	30	**30**	**30**	30	**30**	**30**	25
30	30	30	30	35	30	**35**	**35**	**35**	**35**	**35**	30	**35**	30	30	30	30	30	30	**30**	30	**30**	**30**	30	30	30	35	**30**	30	25
35	30	30	**35**	35	**35**	35	35	**35**	**35**	**35**	30	35	30	30	30	30	30	30	**30**	30	30	30	30	30	30	35	30	**35**	25
35	**35**	**35**	**35**	35	**35**	35	35	**35**	**35**	35	30	35	35	**35**	**35**	**35**	30	30	30	30	30	**35**	**35**	30	30	35	30	35	25
35	35	**35**	35	**40**	35	40	35	**35**	35	35	**35**	35	35	35	**35**	35	**35**	**35**	**35**	35	30	35	35	**35**	35	40	**35**	35	25
40	35	35	35	40	40	40	40	35	35	35	35	35	40	35	35	35	**35**	35	35	35	**35**	35	35	35	**40**	40	35	**45**	**30**
40	50	**40**	50	45	40	40	40	45	35	35	35	35	45	40	35	40	35	35	40	50	35	40	40	40	50	50	35	50	30

Slander treatment sessions – prices offered and purchase prices for every round

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
0	**5**	**5**	0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
5	**10**	**5**	**5**	0	0	**0**	**0**	0	0	**0**	**0**	0	0	**5**	**5**	0	**0**	**0**	**0**	**0**	0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
10	**10**	**10**	**5**	**5**	**5**	**0**	0	0	**5**	**0**	**5**	0	**5**	**5**	**5**	**5**	**5**	0	**0**	0	0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
10	**10**	**10**	**10**	**5**	**5**	**0**	**5**	**5**	**5**	**5**	**5**	0	**5**	**5**	**5**	**5**	**5**	**5**	0	**5**	0	**5**	**5**	**0**	**0**	0	**0**	**0**	0
15	**15**	**15**	**10**	**5**	**5**	**5**	5	**5**	**5**	**5**	5	**5**	**5**	5	**5**	**5**	5	**5**	**5**	**5**	**5**	**5**	5	**5**	0	0	0	0	0
20	**15**	**15**	10	5	**10**	**5**	5	**5**	**5**	**5**	**10**	**5**	**5**	5	5	**5**	5	**5**	**5**	**5**	**5**	**5**	5	5	0	**5**	0	0	**5**
25	15	**15**	10	**10**	**10**	5	**10**	5	5	5	**10**	**5**	**5**	5	5	5	**10**	**5**	5	**5**	**5**	5	5	5	**5**	**5**	0	0	**5**
25	15	**15**	**15**	10	**10**	5	**10**	**10**	5	**10**	**10**	**5**	5	**10**	5	5	**10**	5	5	**5**	**5**	5	5	5	5	**5**	**5**	**5**	5
25	15	15	**15**	**15**	10	**10**	**15**	**10**	**10**	**10**	**10**	5	5	**10**	5	**10**	**10**	**10**	5	5	**5**	5	5	5	5	5	**5**	**5**	**10**
25	**20**	15	**20**	**15**	10	10	**15**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	5	**10**	**10**	**10**	**10**	5	5	5	**10**	**10**	5	5	5	5	**10**
25	20	**20**	**20**	15	**15**	15	**15**	**10**	**10**	10	10	**10**	**10**	**10**	**10**	**10**	10	10	**10**	5	**10**	**10**	**10**	**10**	**10**	5	**10**	5	**10**
25	20	**20**	20	15	**15**	15	**15**	10	10	10	10	**10**	**10**	**10**	**10**	**10**	10	**15**	**10**	**10**	**10**	**10**	10	**10**	**10**	**10**	**10**	5	10
25	**25**	**20**	20	15	**15**	**20**	**15**	**15**	**15**	10	**15**	**10**	**10**	**10**	**10**	10	10	**15**	10	**10**	**10**	10	10	**10**	10	**10**	**10**	**10**	**15**
25	**25**	20	20	15	15	**20**	**15**	**15**	**15**	**15**	**15**	10	**10**	**10**	**10**	10	10	15	10	10	10	10	**15**	10	10	10	**10**	**10**	15
25	**25**	20	**25**	**20**	15	**20**	15	**15**	**15**	**15**	15	10	10	10	10	10	**15**	15	**15**	10	10	**15**	**15**	10	10	**15**	10	**10**	15
25	25	**25**	**25**	**20**	**20**	20	15	**15**	**15**	15	15	**15**	10	10	10	**15**	15	**20**	**15**	10	10	**15**	**15**	10	**15**	**15**	10	10	15
25	25	**25**	**25**	**20**	**20**	20	**20**	**15**	**15**	15	15	**15**	10	10	10	**15**	15	**20**	**15**	**15**	**15**	15	15	10	**15**	15	**15**	**15**	15
25	25	25	25	**20**	20	20	**20**	15	**15**	15	15	**15**	**15**	**15**	10	**15**	15	**20**	15	**15**	**15**	15	**20**	**15**	15	15	15	**15**	**20**
30	**30**	25	25	**20**	20	20	20	15	15	15	15	15	**15**	**15**	10	15	15	**20**	15	**15**	**15**	15	**20**	15	**20**	**20**	15	15	**20**
30	**30**	25	25	**20**	20	20	20	20	**20**	**20**	15	15	**15**	15	**15**	15	15	20	15	15	15	15	20	15	**20**	**20**	**20**	15	**20**
30	**30**	25	25	20	**25**	**25**	20	20	20	**20**	**20**	15	**15**	15	**15**	**20**	**20**	20	**20**	15	15	**20**	20	15	20	20	20	15	20
30	**30**	25	25	20	**25**	**25**	20	20	20	**20**	**20**	**20**	15	15	**15**	**20**	**20**	20	**20**	20	15	**20**	20	**20**	20	20	20	**20**	20
30	30	25	25	**25**	25	**25**	20	20	20	20	**20**	**20**	20	**20**	15	**25**	**20**	**25**	20	20	**20**	**20**	20	**20**	20	20	20	**20**	20
30	30	**30**	30	**25**	25	25	**25**	20	**25**	20	20	**20**	20	20	**20**	25	20	25	**25**	20	20	**20**	20	20	**25**	20	**25**	**25**	20
35	30	30	30	25	25	25	30	**25**	25	20	20	20	20	20	20	25	**25**	25	25	20	**25**	20	**25**	**25**	25	**25**	**25**	25	**25**
35	30	30	30	25	30	25	30	**25**	25	20	**25**	20	20	20	**25**	25	**25**	25	25	**25**	**25**	20	**25**	**25**	**30**	25	25	25	**25**
35	**35**	30	30	25	30	**30**	30	25	25	25	25	20	25	25	**25**	**30**	**25**	**30**	25	**25**	25	20	25	25	**30**	25	25	**30**	**25**
35	**35**	**35**	**35**	**30**	30	**30**	30	30	35	25	25	25	30	**30**	**30**	30	25	30	**30**	**30**	25	**25**	25	25	**30**	**30**	25	30	25
35	35	35	**40**	30	30	30	**35**	30	35	25	25	30	30	30	30	30	30	30	30	**30**	**30**	25	**30**	**30**	30	**30**	**30**	30	**30**
40	35	35	**40**	35	**35**	**35**	35	**35**	40	**35**	30	**35**	**35**	**35**	30	35	35	35	30	30	30	25	**30**	**30**	**35**	**30**	**30**	30	30
40	35	35	**40**	40	45	40	35	40	50	**35**	**35**	35	35	35	**35**	45	**40**	40	**35**	30	30	**30**	30	30	35	30	35	30	40
45	50	**40**	40	45	45	50	**40**	40	50	35	35	40	40	50	45	45	40	40	35	35	30	30	**35**	30	45	40	40	30	45

Sybil treatment sessions – prices offered and purchase prices for every round

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
5	**10**	**5**	**10**	**10**	**5**	**0**	0	**5**	**5**	**5**	**0**	**10**	5	**0**	**0**	**0**	**0**	**0**	**5**	**5**	**0**	**0**	**0**	**0**	**0**	**5**	**0**	**5**	0
10	**10**	**10**	**10**	**10**	**5**	**5**	0	5	**5**	5	0	**10**	5	**0**	**0**	5	**5**	**5**	**5**	**5**	**5**	**0**	0	0	**0**	**5**	0	**5**	**5**
10	**10**	**10**	10	10	5	5	**5**	**10**	5	**10**	5	**10**	**10**	**5**	**5**	**10**	5	**5**	5	**5**	**5**	**5**	0	**5**	0	**5**	**5**	**5**	**5**
10	**10**	10	10	**15**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	10	**10**	**10**	5	**10**	5	**10**	**10**	5	**5**	5	**5**	**5**	**5**	**5**	**5**	**5**	**5**
10	10	10	**15**	**15**	**10**	**10**	**10**	10	**10**	**10**	**10**	10	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	5	5	5	**5**	**10**	**5**	**5**	**5**
15	10	**15**	**15**	**15**	**10**	10	**10**	10	**10**	**10**	**10**	10	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	5	**10**	5	**10**	**5**	**5**	5
15	10	**15**	**15**	15	**15**	10	**10**	**15**	10	**10**	**10**	**15**	10	**10**	**10**	10	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	5	5	**10**
15	**15**	**15**	15	15	**15**	**15**	10	**15**	10	10	**10**	**15**	10	10	**10**	10	**10**	10	**10**	10	10	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**
15	15	15	15	**20**	**15**	**15**	10	**15**	10	10	**10**	**15**	10	10	**10**	10	10	10	10	10	10	**10**	**10**	10	**10**	**10**	**10**	**10**	**10**
20	15	15	15	20	15	**15**	**15**	15	**15**	**15**	**10**	15	**15**	10	10	10	10	10	10	10	10	10	**10**	10	**10**	10	**10**	10	**10**
25	15	**20**	15	20	15	15	**15**	15	**15**	**15**	10	15	**15**	10	10	**15**	**15**	**15**	**15**	10	**15**	10	10	10	10	10	**10**	10	**10**
25	**20**	**20**	**20**	20	**20**	15	**15**	15	15	15	10	15	**15**	10	10	**15**	**15**	**15**	**15**	10	**15**	10	10	10	10	10	**10**	10	**10**
25	20	20	**20**	20	**20**	15	**15**	**20**	15	**20**	15	15	**15**	10	10	**15**	**15**	**15**	**15**	10	15	10	**15**	**15**	10	15	10	10	10
25	20	**25**	**20**	20	**20**	15	15	**20**	**20**	20	15	15	15	**15**	**15**	**15**	15	15	15	**15**	15	**15**	**15**	**15**	10	**15**	10	10	10
25	20	**25**	20	**25**	**20**	**20**	15	20	**20**	20	15	**20**	**20**	**15**	15	**15**	15	15	15	**15**	**20**	**15**	**15**	**15**	10	**15**	10	**15**	10
25	**25**	**25**	20	**25**	20	**20**	15	**25**	**20**	20	20	**20**	**20**	15	15	15	15	15	15	15	**20**	**15**	15	**15**	10	15	10	**15**	10
25	**25**	25	**25**	**25**	20	20	15	**25**	**20**	20	20	20	20	15	15	15	15	**20**	15	15	**20**	15	**20**	**20**	**15**	15	**15**	**15**	10
25	**25**	25	**25**	25	20	20	15	**25**	20	**25**	20	20	20	**20**	**20**	**20**	15	**20**	15	15	**20**	**20**	**20**	**20**	15	**20**	**15**	15	**15**
25	25	25	**25**	25	**25**	**25**	15	25	20	**25**	**25**	20	**25**	**20**	**20**	**20**	15	20	**20**	15	20	**20**	20	**20**	15	20	**20**	15	**15**
30	25	25	**25**	25	**25**	**25**	**20**	25	20	**25**	**25**	20	**25**	20	20	20	**20**	20	**20**	**20**	20	20	20	20	**20**	20	**20**	**20**	**15**
30	25	**30**	**25**	25	25	25	20	25	**25**	**25**	**25**	**25**	25	20	20	20	**20**	20	20	20	**25**	20	**25**	20	**20**	20	20	**20**	15
30	25	**30**	25	**30**	25	25	**25**	25	**25**	25	**25**	**25**	25	20	20	20	20	**25**	20	20	25	**25**	**25**	20	20	**25**	20	20	**20**
30	25	30	25	**30**	25	**30**	25	25	25	**30**	25	25	25	**25**	**25**	20	**25**	**25**	20	**25**	25	25	25	25	**25**	25	20	**25**	**20**
30	**30**	30	30	**30**	25	30	25	**30**	**30**	**35**	25	**30**	**30**	**25**	**25**	**25**	**25**	25	25	**25**	25	25	25	25	25	25	20	25	20
30	30	30	30	**30**	25	**35**	**30**	**30**	30	**35**	25	**30**	30	25	25	25	25	30	25	25	25	25	30	25	25	**30**	25	25	20
35	30	**35**	**35**	**35**	**30**	**35**	**30**	30	30	35	25	**30**	30	25	30	25	**30**	**35**	**30**	**30**	**30**	**30**	30	**30**	**30**	**30**	25	**30**	25
35	**35**	**35**	**35**	35	30	35	30	**35**	30	35	**30**	**35**	30	25	30	**30**	**35**	35	**35**	**35**	**35**	**30**	30	**30**	**35**	30	**30**	30	25
40	**35**	40	35	35	30	**40**	30	35	**35**	35	30	**35**	**35**	**30**	**35**	30	**35**	40	**35**	**35**	35	30	**35**	**35**	**35**	**35**	30	30	**30**
40	35	40	35	**40**	35	45	**35**	35	**35**	35	**35**	35	**35**	**35**	35	**35**	35	40	**35**	**35**	35	**35**	**35**	35	35	35	**35**	**35**	30
40	**40**	40	**40**	40	35	45	35	35	35	40	**35**	**40**	35	**35**	**40**	**35**	35	40	35	35	40	35	35	35	35	35	35	35	35
45	**40**	**45**	40	40	**40**	45	**40**	**40**	40	40	**35**	45	35	35	40	35	35	**45**	45	35	45	35	**40**	40	40	35	35	35	40
50	45	45	50	**45**	45	**50**	**40**	**40**	45	45	35	45	**40**	40	**45**	40	40	50	50	**40**	50	40	45	40	40	35	35	50	45

Number of product qualities offered for every round across treatments

	Control sessions			Slander treatment sessions			Sybil treatment sessions		
Round number	**Low**	**Medium**	**High**	**Low**	**Medium**	**High**	**Low**	**Medium**	**High**
1	6	11	11	5	19	8	9	18	5
2	5	14	9	10	12	10	12	14	6
3	8	10	10	12	11	9	11	13	8
4	7	10	11	10	8	14	7	14	11
5	3	12	13	16	10	6	4	17	11
6	6	11	11	13	7	12	9	13	10
7	4	14	10	11	14	7	8	12	12
8	6	7	15	14	9	9	10	11	11
9	5	10	13	14	10	8	8	14	10
10	5	10	13	14	9	9	11	9	12
11	4	9	15	10	15	7	10	10	12
12	7	9	12	11	16	5	8	12	12
13	6	9	13	14	8	10	8	12	12
14	7	6	15	15	10	7	8	13	11
15	9	9	10	15	9	8	10	12	10
16	6	11	11	15	8	9	10	11	11
17	5	12	11	13	7	12	13	11	8
18	10	6	12	11	11	10	9	13	10
19	5	12	11	8	12	12	10	13	9
20	7	13	8	12	8	12	12	12	8
21	7	12	9	10	9	13	11	13	8
22	6	10	12	13	8	11	8	14	10
23	7	11	10	10	13	9	11	11	10
24	5	10	13	12	11	9	9	14	9
25	8	11	9	13	8	11	9	13	10
26	7	11	10	12	8	12	12	9	11
27	8	8	12	13	11	8	12	11	9
28	8	11	9	15	7	10	10	12	10
29	9	8	11	16	8	8	12	12	8
30	12	10	6	17	5	10	14	9	9

Appendix D.4 – Trust games amounts sent and sent back by all participants across sessions

Results of the trust games are presented below, including numbers of tokens sent and sent back by every participant for every treatment. The number of tokens presented varies between sessions because the Control sessions had 6 fewer participants.

Control				Slander treatment				Sybil treatment			
Sent 1	**Sent 2**	**Back 1**	**Back 2**	**Sent 1**	**Sent 2**	**Back 1**	**Back 2**	**Sent 1**	**Sent 2**	**Back 1**	**Back 2**
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	5	0	0	0	10	5	0	0
5	0	0	0	5	0	0	0	10	5	0	0
5	0	0	0	5	0	0	0	10	5	0	0
5	0	0	0	5	0	0	0	10	5	0	0
5	5	0	0	10	0	0	0	10	10	0	0
5	5	0	0	10	0	0	0	10	10	0	0
10	10	0	0	10	5	0	0	10	10	0	0
10	10	0	0	10	5	0	0	10	10	0	0
10	10	5	0	10	5	0	0	10	10	0	0
10	10	5	0	10	5	0	0	10	10	0	0
10	10	5	0	10	10	5	0	10	10	5	5
10	10	5	0	10	10	5	0	10	10	5	5
10	10	10	0	15	10	5	0	15	10	5	5
10	10	10	0	15	10	5	0	15	10	5	5
10	10	10	0	15	10	5	0	15	10	15	15
10	10	10	0	15	10	5	0	15	10	15	15
15	10	10	5	15	10	10	5	15	10	15	15
15	10	10	5	15	10	10	5	15	10	15	15
15	15	15	10	15	15	10	5	15	10	15	15
15	15	15	10	15	15	10	5	15	10	15	15
15	15	20	10	20	15	10	5	15	15	15	20
15	15	20	10	20	15	10	5	15	15	15	20
20	15	20	15	20	15	10	10	15	15	20	20
20	15	20	15	20	15	10	10	15	15	20	20
20	15	20	20	20	20	15	15	15	15	20	20
20	15	20	20	20	20	15	15	15	15	20	20
20	20	20	20	25	20	20	15	15	15	20	20
20	20	20	20	25	20	20	15	15	15	20	20
25	25	30	25	25	20	20	20	15	15	20	20
25	25	30	25	25	20	20	20	15	15	20	20
25	25	30	30	25	25	20	20	20	15	20	20
25	25	30	30	25	25	20	20	20	15	20	20
25	25	40	30	25	25	25	25	20	25	20	20
25	25	40	30	25	25	25	25	20	25	20	20
25	25	50	50	25	25	30	25	25	25	25	25
25	25	50	50	25	25	30	25	25	25	25	25
				25	25	35	25	25	25	30	30
				25	25	35	25	25	25	30	30
				25	25	35	30	25	25	30	35
				25	25	35	30	25	25	30	35
				25	25	40	30	25	25	50	50
				25	25	40	30	25	25	50	50

Appendix D.5 – Survey results

FEMALE	MALE
54%	46%

UNDERGRADUATE	POSTGRADUATE TAUGHT	POSTGRADUATE RESEARCH
54%	19%	27%

HUMANITIES	SOCIAL SCIENCES	SCIENCE AND MEDICINE
20%	42%	38%

I got to know and trust other participants I was trading with – (Strongly disagree) 1 – 5 (Strongly agree)

	CONTROL	SLANDER	SYBIL
DISAGREE (1-2)	61%	65.9%	41.7%
NEUTRAL (3)	22%	14.9%	41.7%
AGREE (4-5)	17%	19.2%	16.6%

I distrusted other participants – (Never) 1 – 5 (Always)

	CONTROL	SLANDER	SYBIL
NEVER (1-2)	26.8%	23.4%	31.3%
NEUTRAL (3)	22%	23.4%	35.4%
ALWAYS (4-5)	51.2%	53.2%	33.3%

I still traded with participants I distrusted – (Never) 1 – 5 (Always)

	CONTROL	SLANDER	SYBIL
NEVER (1-2)	17%	8.5%	10.5%
NEUTRAL (3)	36.6%	34%	31.2%
ALWAYS (4-5)	46.4%	57.5%	58.3%

I exhibited trustworthy behaviour to other participants – (Strongly disagree) 1 – 5 (Strongly agree)

	CONTROL	SLANDER	SYBIL
DISAGREE (1-2)	12.2%	19.1%	10.4%
NEUTRAL (3)	7.3%	14.9%	14.6%
AGREE (4-5)	80.5%	66%	75%

The rating mechanisms encouraged me to exhibit trustworthy behaviour – (Strongly disagree) 1 – 5 (Strongly agree)

	CONTROL	SLANDER	SYBIL
DISAGREE (1-2)	9.8%	23.5%	12.5%
NEUTRAL (3)	12.3%	8.5%	29.1%
AGREE (4-5)	78.2%	68%	58.4%

I do not like to take risks – (Strongly disagree) 1 – 5 (Strongly agree)

	CONTROL	SLANDER	SYBIL
DISAGREE (1-2)	36.6%	48.9%	43.7%
NEUTRAL (3)	29.3%	14.9%	18.8%
AGREE (4-5)	34.1%	36.2%	37.5%

My decisions were based solely on profit-seeking – (Strongly disagree) 1 – 5 (Strongly agree)

	CONTROL	SLANDER	SYBIL
DISAGREE (1-2)	41.5%	19.2%	41.7%
NEUTRAL (3)	14.6%	19.1%	12.5%
AGREE (4-5)	43.9%	61.7%	45.8%