The Role of Informal Workers in Online Economic Crime

By

Masarah-Cynthia Paquet-Clouston

M.A. (Hons.), Université de Montréal, 2017

B.A., Université Laval, 2013

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Doctor of Philosophy

in the
School of Criminology
Faculty of Arts and Social Sciences

SIMON FRASER UNIVERSITY

Fall 2021

Declaration of Committee

Name:	**Masarah-Cynthia Paquet-Clouston**
Degree:	**Doctor of Philosophy (Criminology)**
Title:	**The Role of Informal Workers in Online Economic Crime**
Committee:	**Chair:** **Bryan Kinney** Associate Professor, Criminology
	Martin Bouchard Supervisor Professor, Criminology
	Richard Frank Committee Member Associate Professor, Criminology
	Eric Beauregard Committee Member Professor, Criminology
	Kevin Schnepel Examiner Assistant Professor, Economics
	Edward Kleemans External Examiner Professor, Faculty of Law, Criminology Vrije Universiteit Amsterdam

Ethics Statement

The author, whose name appears on the title page of this work, has obtained, for the research described in this work, either:

a. human research ethics approval from the Simon Fraser University Office of Research Ethics

or

b. advance approval of the animal care protocol from the University Animal Care Committee of Simon Fraser University

or has conducted the research

c. as a co-investigator, collaborator, or research assistant in a research project approved in advance.

A copy of the approval letter has been filed with the Theses Office of the University Library at the time of submission of this thesis or project.

The original application for approval and letter of approval are filed with the relevant offices. Inquiries may be directed to those authorities.

Simon Fraser University Library
Burnaby, British Columbia, Canada

Update Spring 2016

Abstract

Context: Online economic crime leverages information technologies (IT) for illegal wealth redistribution, such as banking theft. Such crime requires a series of actions, a scheme, to be successful. Informal workers, individuals whose economic activities escape regulations, can be leveraged to execute various tasks surrounding these schemes. However, what these workers represent for online economic crime organizations, and their impact on the reach and sophistication of the crime, has yet to be uncovered. This thesis focuses on understanding the contexts, motivations, and organizations of those behind online economic crime. While doing so, it assesses the role and availability of an informal IT workforce surrounding the crime organization and its likelihood to participate in such criminal schemes.

Methods and Data: This thesis builds on three data sources: (1) 21 semi-structured interviews with experts, (2) a private chat log containing discussions among individuals involved in online economic crime, and (3) two datasets on an informal IT workforce operating on a digital labor platform. A blend of qualitative and quantitative analyses is developed, including inductive thematic analysis, non-parametric statistical hypothesis tests, and group-based trajectory modeling.

Results: The findings illustrate three key contextual factors influencing those behind online economic crime: a lack of legal economic opportunities, a lack of deterrents and the availability of drifting means. Organizations behind online economic crime are found to take various forms, from organized, to enterprise-like, loose networks or communities. They are also characterized by a large sphere of influence given the indispensable workers hired to help with the crime orchestration. Among them, informal workers from the IT sector are found to be particularly important: they represent a pool of potential workers for all legal tasks surrounding online economic crime, and they can be leveraged easily due to digital labor platforms. However, further investigations illustrate that the benefits of hiring informal IT workers may be hindered by high transaction costs, including high hiring, switching, and monitoring costs. Moreover, the likelihood of informal IT workers to participate in crime-oriented spaces is found to be limited.

Conclusion: This study sheds light on the organization of online economic crime and the role of informal IT workers at the periphery. It provides both theoretical and empirical explanations as to why online economic crime is characterized by long reach, in terms of victims, and sophistication. It also offers nuanced concepts (e.g., drifters, informal workforce) to better grasp the organization of online economic crime and the degrees of involvement of those surrounding the crime.

Acknowledgements

First and foremost, Martin, what a ride! Ever since I contacted you on Twitter because I was interested in doing a PhD with you all the way up to moving to Vancouver and then Prague, you have always been there. You opened my mind to new theories and methods while giving me just enough flexibility to find my own path. From developing the collective broker measure to measuring cannabis consumption trends or talking about the drifting concept, I had a blast in the past years with you, both intellectually and socially. Most people are happy when their PhD is done. I am. But I must admit I could have continued a long way with you. As my mentor and friend, I truly hope we keep on working together.

Sebastian, Vero, Mariko, Ondrej and MaryJo, I don't think I can thank you enough. You have been a family to me, but also an inspiration. I am still wondering how a Lab can mix so many curious, passionate, authentic, and incredibly smart people. I feel privileged to have been part of your group. From conducting amazing interviews to drinking pivo, eating empanadas or chillin' on a boat, I would change nothing. If you are reading this, I am winking at you now ;).

Lorne, mentor and friend, thank you. You have helped for how long now? 12 years. How lucky am I to have you! I will always remember the last miles of writing, when you were fully available to answer my never-ending English questions. You stabilized me, provided me with the pillars I needed to continue. You had my back, and I owe you for that. Thank you also for being my friend, sharing your passions, readings, and experiences with me. I'm sure we still have many more years of discussions to come, and this makes me smile.

There are also many friends I want to thank, friends who have been there in the past years: Cyndi (ce que tu as fait pour moi au moment où j'en avais le plus besoin, je te suis 100% reconnaissante), Olivier, Laurent, Alice (ma chum d'amour) and Anna. Carlo, I miss you.

Finally, there's Sergovi. You entered my life unexpectedly and now I cannot picture it without you. Sergovi, I thank you for sharing and supporting my crazy ideas, keeping up with my *mono-sujets*, learning Czech and discovering Prague with me. I hope we have many more years of dancing, drinking pivo, courir sur des roches and

building an empire of theories and methodologies that will help us better understand the world we share together.

Finally, I thank the Grand Monarque et les vacances de l'esprit. These past years have been memorable. Děkuji all!

Table of Contents

List of Tables

List of Figures

Chapter 1. **Introduction**

Information technologies[1] (ITs) have become a central component of everyday life and, with them, new crime opportunities have emerged, especially profit-driven crime opportunities. ITs connect individuals all around the world in an instant, providing diffusion capabilities beyond geographic borders. Such contraction increases the number of crime opportunities, as individuals do not need to physically move to commit a crime and can target multiple victims at the same time (Llinares and Johnson, 2018; Leukfeldt and Yar, 2016; Yar, 2005). These opportunities are appealing up to the point that Anderson et al. (2019) estimated that, nowadays, half of profit-driven crimes are happening online.

ITs also influence the organization behind criminal activities. For example, crime-related products and services can be traded and new business partnerships can be established (Leukfeldt, Kleemans and Stol, 2017d). In addition, a large number of workers offer their services online (Schmidt, 2017; Drahokoupil and Fabo, 2016; Drahokoupil and Piasna, 2017), and these services can be used for criminal purposes without their necessarily knowing. Indeed, the neutrality (or detachment) of many tasks achieved through IT creates a grey area that can be leveraged by those orchestrating online criminal schemes (Leukfeldt et al., 2020; Bijlenga and Kleemans, 2018).

So far, extant research has investigated the organization of criminal groups involved in IT-related profit-driven crime, known as *profit-driven cybercrime*. However, profit-driven cybercrime is a wide concept, mixing both online market transactions (e.g., sale of an illicit product) and illegal redistribution of wealth (e.g., theft). This thesis focuses only on the former, online economic crime, which refers to illegal wealth distribution through online means. Examples of online economic crime include ransomware attacks or credit card thefts.

Online economic crime is characterized by its long reach in terms of number of victims (Tcherni et al., 2016). Moreover, several online economic crime schemes, such as sextortion spam (Paquet-Clouston et al., 2019), banking theft (Kuraku and Kalla

[1] Information technologies can be defined as any technologies "used to acquire, store, organize and process data as well as disseminate processed data which can be used in specified applications" (Rajaraman, 2018, p.17).

2020, Garcia et al., 2019), or ransomware (Paquet-Clouston et al., 2018; Huang et al., 2018) involve targeting as many people (or companies) as possible to increase the chances of successfully stealing money. The crime is also characterized by sophistication (as opposed to street wallet theft); it requires several steps to be successful, from enticing a user to click on malicious links to compromising a bank account, all the way up to money laundering (Leukfeldt, Kleemans and Stol, 2017c).

Despite the international nature of ITs, organizations involved in online economic crime have been found to be locally embedded. Their structure also resembles that of traditional criminal groups (Leukfeldt et al., 2020; Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a,b,c; Leukfeldt, 2014). Still, much has to be uncovered on the contexts, motivations, and organizations of those behind such crime. This is especially true considering that many aspects surrounding online economic crime, such as building websites, resemble licit activities in the IT sector. Already, the involvement of a necessary class of IT workers in activities surrounding online economic crime has been mentioned in several studies (Collier et al., 2020; Leukfeldt et al., 2019; Bijlenga and Kleemans, 2018; Leukfeldt, Kleemans and Stol, 2017a,b,c,d).

Moreover, to recruit IT workers, there exist online digital labor platforms: unregulated spaces that host a large pool of IT workers at a very low cost (Schmidt, 2017; Drahokoupil and Fabo, 2016; Drahokoupil and Piasna, 2017). Due to their unregulated status, a lot of work taking place through them can be considered as *informal*: the means by which a product or a service is produced and distributed takes place outside the law (Castell and Porter, 1989). Just like in traditional informal markets, these informal spaces represent attractive settings for criminal organizations (Sabet, 2015). Already, a small number of studies have shown that some of the tasks offered on digital labor platforms are related to shady activities (Farooqi et al., 2017; Garg, Camp and Kanich, 2013; Motoyama et al., 2013). What these workers represent for online economic crime organizations, and their impact on the reach and sophistication of the crime, has yet to be uncovered. Such an assessment may yield insights on various avenues to deter and prevent such crime by motivated offenders, but also by informal IT workers involved at the periphery of the crime.

This thesis focuses on understanding the contexts, motivations, and organizations of those behind online economic crime. While doing so, it assesses the role and availability of an informal workforce surrounding the crime organization and its likelihood to participate in these criminal schemes. To this end, three sources of data are used: (1) 21 semi-structured interviews with experts, (2) a chat log containing private discussions among individuals involved in online economic crime, and (3) two quantitative datasets of an informal workforce operating on a digital labor platform.

In the first part of the thesis, the two qualitative sources of data (interviews and private chat log) are used to uncover the contexts, motivations, and organizations of those behind online economic crime. From these analyses, the importance of informal IT workers in the orchestration of the crime is uncovered. Consequently, the second part of the thesis uses two quantitative datasets on an informal IT workforce to assess its relationship between informal and crime-oriented spaces.

The thesis starts by presenting, in **Chapter 2**, a review of relevant empirical research on the topic, which includes studies on the organization of criminal groups and those behind profit-driven cybercrime as well as studies on informal markets and digital labor platforms. The theoretical frameworks used are outlined: Reuter's (1983) study on the consequences of product illegality, Naylor's (2003) profit-driven cybercrime, and Matza's (1990) drift concept. Then, **Chapter 3** outlines the research objectives and questions. A figure with the thesis workflow is also provided. Two objectives lead this thesis; each of them is answered with two analyses.

The first objective is to uncover the contexts and motivations that may drive individuals to participate in online economic crime. Twenty-one semi-directed interviews are conducted with experts knowledgeable on the topic. The methods and data are presented in **Chapter 4**. Then, **Chapter 5,** entitled *Experts' Perceptions: Contexts, Motivations and Organizations,* presents the results. The analysis uncovers three contextual factors that influence individuals to participate in online economic crime: a lack of legal economic opportunities, a lack of deterrents, and drifting means. Their confluence in a specific setting is likely to predict the presence of a large population of individuals involved in online economic crime. In terms of potential motivators mentioned by experts, financial gains and feelings (including pride, fame, excitement and power over others) are identified. Financial gain is of no surprise as online economic crime is a

profit-driven crime, but investigating this question led to discovering that only a small proportion of individuals are perceived as successful in their criminal endeavors. Within **Chapter 5**, experts' narratives suggest that the organization behind online economic crime takes many forms, from organized to loosely structured or enterprise-like. Regardless of these structures, individuals involved in online economic crime are dependent on a population of individuals evolving at the periphery, called **indispensable workers**: indispensable as a group, yet dispensable as individuals**.**

Uncovering contexts and motivations behind online economic crime is also achieved by analyzing private conversations among individuals involved in online economic crime. **Chapter 6** presents the methods and data for this analysis. Then the results are presented in **Chapter 7,** entitled: *Private Chats: Dancing on the Crime Line*. In short, the individuals studied are advertising malicious Android applications on their websites on behalf of a criminal group. Their conversations illustrated that they are amateur workers working in IT and facing an adverse business environment. They seek economic independence yet do not achieve it. These individuals are found, in the end, to be the indispensable workers mentioned by experts.

The results of the two qualitative analyses emphasize the existence of **indispensable workers** surrounding online economic crime organization. They are positioned at the periphery of the criminal group, and their mass forms a sphere of economic influence that those orchestrating online economic crime can exploit. One strand of indispensable workers that are key to online economic crime is **informal workers from the IT sector**.

Furthermore, the private conversations analyzed in **Chapters 6 and 7** led to **uncovering a digital labor platform for IT-related products and services**. Digital labor platforms host a pool of potential IT workers for those behind online economic crime. Their presence suggests, a priori, that online economic crime groups could hire a large workforce. Yet, based on insights from the private chat log in **Chapter 7** (coupled with previous research), the benefits of hiring workers online may be mitigated by transaction costs, including hiring costs (e.g., finding the worker with the right skills), switching costs (e.g., costs associated to switching worker afterwards), and monitoring costs (e.g., making sure the job is done).

The benefits may also be limited by informal workers' willingness to participate in criminal activities. To assess this, the digital labor platform uncovered in **Chapters 6 and 7** is leveraged. This platform is called the "informal platform" throughout the thesis. Information on the IT workforce operating on the informal platform is extracted and the concept of **drifter** is developed. Drifters are informal workers who have commented at least once in crime-oriented platforms (e.g., carding, hacking platforms).

The second objective of this study is to assess drifters' relationship between informal and crime-oriented spaces. Drifters are identified in the informal IT workforce. Whether they form a distinctive group is evaluated through a series of non-parametric tests comparing drifters' behaviors on the informal platform with non-drifters. **Chapter 8** presents the methods and data for this quantitative analysis. **Chapter 9,** entitled: *Indistinguishable Drifters,* presents the results, which show that only a small proportion of IT workers are drifters, and they are relatively indistinguishable in the workforce studied based on the indicators developed.

The second objective is also answered through an additional analysis of drifters' posting behavior in the informal platform vs crime-oriented platforms through a nine-year period. Data and methods are presented in **Chapter 10**. The results are presented in **Chapter 11,** entitled: *Drifter Trajectories Favor Informality.* They illustrate that most drifters favor the informal space over crime-oriented ones over time. Overall, drifters' engagement in crime-oriented platforms is limited. Such minimal drift recalls Matza's (1990) statement that drift is transient and rather rare for most individuals.

Chapter 12 provides a discussion of the thesis results. Four discussion points emerge: 1) understanding the underlying forces that influence individuals to participate in online economic crime, 2) exploring their organizations and the role of informal workers involved, 3) illustrating the benefits and difficulties of hiring such a workforce through digital labor platforms, and 4) presenting the workforce's limited involvement in crime-oriented platforms. They are put in relation with the literature on the topic. Study limits and future research are also presented.

The conclusion is presented in **Chapter 13**. Additional follow-up ideas are introduced. One suggests that specific settings where the contextual factors (identified in this thesis) converge may foster large and structured organizations behind online

economic crime. Another idea proposes that the informal workforce uncovered may partly explain the crime's reach and sophistication. A third idea suggests that there is a need to think beyond motivated offenders when studying online economic crime, taking more nuanced approaches. Lastly, further thoughts on how to prevent online economic crime participation (from an informal IT worker perspective) are briefly outlined.

In sum, this study sheds light on the organization of online economic crime and the role of informal workers at the periphery. It provides both theoretical and empirical explanations as to why online economic crime is characterized by long reach, in terms of victims, and sophistication. It also offers nuanced concepts (e.g., drifters, informal workforce) to better grasp the organization of online economic crime and the degrees of involvement of those surrounding the crime.

As the reader might have noticed, the thesis structure differs from that of traditional theses. For each analysis, the methods and data are presented first, followed by the results. This structure is the most efficient one to allow readers to keep track of the various methodological decisions taken and evaluate the results.

Chapter 2.

Theoretical Framework and Empirical Review

As a reminder, this thesis focuses on understanding the contexts, motivations, and organizations of those behind online economic crime. While doing so, it assesses the role and availability of an informal workforce surrounding the crime organization and its likelihood to participate in these criminal schemes.

The *theoretical framework and empirical review* section binds together several strands of literature that are helpful to position the thesis' results in extant literature. The section starts by reviewing what is known on the organization of criminal groups and moves to the organization of those behind profit-driven cybercrime. How online economic crime is conceptualized, based on Naylor's (2003) profit-driven typology, is also presented.

Then, considering the role of informal workers in online economic crime organization, what is known on informal economies and digital labor platforms that gather IT-related workers is subsequently introduced. To understand how and why individuals, such as informal workers, end up participating in crime, Matza's (1990) drift concept and Goldsmith and Brewer's (2015) digital drift idea are finally outlined.

2.1. On the Organization of Criminal Groups

Reviewing the literature on the organization of criminal groups provides insights on the dynamics that influence their size, scope, and structure. These insights can be used to understand the organization of groups behind online economic crime. What, then, is known about the organization of criminal groups?

Similar to popular journalistic depictions of organized crime, Cressey (1969) argued that criminal groups are organized as hierarchical bureaucracies that control the supply of illegal products and services. However, although such bureaucracies do exist, this conceptualization was found to depict outlier cases (Edwards and Levi, 2008; Paoli et al., 2007). Instead, in general, individuals operating in illicit realms are found be

loosely organized. They are known to associate for a few economic transactions and split afterwards (Morselli, 2009; Morselli et al., 2007; Reuter and Haaga, 1989).

Reuter (1983) convincingly outlined how those operating in concealed environments are forced to stay within a small size and scope due to the consequences of product[2] illegality. Indeed, the legal status of the product affects the way in which it is produced and distributed. Reuter's (1983) framework was found to be useful in this thesis to understand various tradeoffs that those behind online economic crime face when developing their schemes. Indeed, although the goal of online economic crime is illegal wealth redistribution, there exists a whole enterprise behind the crime orchestration. A short summary of Reuter's ideas is therefore presented below.

Reuter (1983) argued that since contracts are not enforceable in court law, the asset produced and distributed may be seized by law enforcement. Since all participants face risks of arrest, information on the production and distribution of the product must be controlled. As **employees** represent a major threat to entrepreneurs, the larger the number of employees the higher the risk. In addition, monitoring employees' performance is difficult given that they operate in covert settings (p.117). Thus, having a large pool of employees is unlikely as relationships must be structured around providing little information on the activities of those involved.

For these reasons, the supply process is likely to be fragmented, preventing entrepreneurs from vertically integrating the production process forward or backward which, usually, would allow them to tap into economies of scale and eventually control the provision of the input and its costs (p.120). Moreover, **with limited access to credit**, entrepreneurs do not have access to external credits, nor can they separate ownership and management (as is the case in large legal companies) nor transfer their ownership. Theoretically, the growth of an illegal firm is short and limited to the lifetime of the entrepreneur (p.122).

Reuter (1983) added that entrepreneurs can try to **corrupt** law enforcement for their organizational growth, thus requiring the corrupted police officers to regulate the market and decreasing the risks of arrest. However, if a police structure is complex and

[2] The analysis could also be applied to firms providing illegal services. However, the term "product" is used in the summary for simplicity purposes.

many agencies have power over the entrepreneur's territory, the likeliness of bribing all agencies and getting away with it is low (p.126).

Final customers, such as drug users, of the product represent a significant threat to entrepreneurs: they take few precautions, they are not loyal, they are many, they face few legal consequences, and they represent the starting point for most law enforcement investigations. For these reasons, to prevent contact, the entrepreneur must fragment tasks. Developing customers' goodwill therefore becomes difficult as the customer knows only the person with whom they[3] deal. Advertising the product and creating a brand to develop customer loyalty is thus futile (p.129).

Illegal enterprises also are likely to stay within a small **geographic scope** because they cannot monitor distant agents for performance nor control the hazard associated with transportation and communications. As more borders are crossed, the multiplication of law enforcement agencies potentially investigating the illegal activities increases as well. This, coupled with the inability of the entrepreneur to develop brand loyalty, will prevent an enterprise's geographical growth (p.130).

Lastly, **diversification** of similar products is likely to happen as there is a quick profit margin to be gained by reducing consumers' search costs[4]. Diversification across unrelated product lines is not likely to happen, on the other hand, mainly due to increased exposure. Reuter (1983) concluded that illegal markets are much more competitive than previously thought due to two driving forces: 1) concern for police intervention and 2) lack of enforceable legal contracts. Illegal markets are consequently likely to be populated by localized, fragmented, ephemeral, and undiversified enterprises (p.132).

Bouchard and Morselli (2014) reviewed the literature on the size of criminal organizations and corroborated that criminal organizations are likely to be small. The authors found that they are typically formed of fewer than 10 individuals, a pattern that emerges across time, space and markets. More precisely, the size of criminal organizations follows a power-law distribution with the majority of groups being small (from 2 to 5, fewer than 10) and a few representing large groups, the most visible ones

[3] "They" is used to avoid gender-specific phrasing throughout the thesis.

[4] Refers to opportunity costs associated with searching for a product.

(p.294). However, the authors highlighted that small groups often loosely collaborate with ongoing criminal networks, which does not require the participation of all group members. This raises questions on the conceptualization around the size and scope of organizations beyond direct membership, as discussed below.

2.1.1. Boundary Specification Beyond Group Membership

The concept of “economic influence” brought forth in Tremblay, Bouchard and Petit (2009), conceptualizes criminal organization less as a strict group with specific membership statuses, but more as a network of individuals interdependent on one another yet embedded within a criminal market. Economic influence is not an attribute of a criminal organization, but rather a relational outcome; it captures the effect of a criminal group outside of its specified boundaries (p.4-5). The authors conclude that a small organization of about 100 individuals can have a relatively large sphere of economic influence, reaching thousands of individuals working in the market or in its periphery.

Consequently, criminal groups are organized through “a resource pooling process that is built around individuals who are socially embedded in various ways beyond co-membership in a criminal organization” (Bouchard and Morselli , 2014, p.298-299). Opportunistic structures constitute a better configuration of criminal organizations, opportunisitic because 1) criminal organizations lack history or reputation; 2) they are small at the operative level; and 3) they lack sophisticated internal organization (Bouchard and Morselli, 2014, p.294).

Within the sphere of influence of criminal groups, a multitude of legitimate actors are involved in various parts of the supply chain, such as transporters, corrupted officials, investors, lawyers, and accountants (Morselli and Giguère, 2006; Lyman and Potter, 2001). These actors are known as **facilitators** and defined as participants, from the legitimate realm, who provide operational services to individuals involved in criminal activities (for a review, see Morselli and Giguère, 2006). For example, Bouchard and Dion (2012) reported legitimate shops that provided cannabis cultivators with proper equipment. Facilitators provide legitimate status, business experience, financial capital, and logistical resources to criminal organizations, while even sometimes filling key roles in criminal ventures (Morselli and Giguère, 2006).

These individuals may end up involved in criminal organizations due to social opportunity structures, where individuals in the direct social environments of those involved in the criminal activities are drawn into these activities (Kleemans and De Poot, 2008; Kleemans and van de Bunt, 2003; Kleemans and Van de Bunt, 1999). Kleemans and De Poot (2008) identified five mechanisms that explain why individuals may end up involved in criminal groups: 1) existing social ties, 2) work and profession, 3) leisure activities and sidelines, 4) life events and 5) being recruited. Whether these individuals may end up involved in criminal groups may also depend on various contextual factors.

This raises the question: what contextual factors influence the growth of an organization? The conclusion that criminal organizations are small in size, and scope compares the size of such organizations with legal ones (Bouchard and Ouellet, 2011). The variation in organization size, once the consequence of product illegality is considered, may depend on various characteristics, such as the type of product traded or the pool of individuals willing to associate. The optimal size of a criminal organization is a product of its environment (Bouchard and Ouellet, 2011; Donaldson, 2001). Looking at the literature on shifts and patterns in the mobility of criminal groups can offer information on the factors influencing their size and scope..

2.1.2. Contextual Factors Influencing the Size of Criminal Organizations

Morselli, Turcotte and Tenti (2011) reviewed past studies to examine what influences shifts and patterns in the mobility of criminal groups. They identified various push (driving individuals out of a setting) and pull (drawing individuals to a setting) factors that may influence group patterns across a variety of settings.

Pull factors create criminogenic environments and offer a high volume of interesting illegal opportunities; seven were identified: mass demand, access to supply, lax law enforcement, high impunity/corruption, proximity to trafficking routes, porous borders, and the presence of brokers and facilitators. In short, mass demand and mass supply create market opportunities while lax law enforcement and high impunity/corruption allow individuals to believe that they will not face the consequences of their actions. Trafficking routes and porous borders matter for specific illegal products such as drugs while the presence of brokers and facilitators often helps the criminal

organization with market segmentation and dealing with what the authors call “ordinary citizens”.

Only two push factors, driving individuals outside of a criminal setting, were subsequently identified: increased law enforcement and increased competition from criminal groups. These two factors could lead individuals to stop their criminal activities, either due to risks of arrest or due to the meager profit yielded by these activities. Paoli, Greenfield and Reuter (2009) also provided an explicit proposition that law enforcement effectiveness has a direct impact on the size of criminal organizations.

Morselli, Turcotte and Tenti (2011) differentiated between the strategic context, where individuals organize around available opportunities, and the emergent context, where opportunities influence individuals to organize. However, their main conclusion was that opportunities matter more than the group itself in explaining growth and mobility in criminal groups, as the problems concerning locations and markets are persistent through time while the groups exploiting them are small and transient (p.165).

Tremblay, Cusson and Morselli (1998) identified three arguments that may explain the limits to growth of criminal organizations: 1) the consequences of product illegality, 2) unequal availability of corruption opportunities in various settings and jurisdictions, and 3) social norms/moral condemnation. As the consequence of product illegality was already discussed above, only the two other arguments are briefly outlined below. Unequal availability of corruption opportunities refers to the uncertainty and difficulty of successfully bribing law enforcement agents across time and space. Corrupted agents may yield impunity to individuals, and subsequent organizational growth, but maintaining relationships via corruption is relentless and uncertain. Social norms and moral censure refer to the degree of moral acceptance, in a society, of the organizational criminal activities.

When the illegal product or service is widely condemned socially (e.g., human trafficking or the trading of human organs), those trading it will face additional constraints, such as having to hide not only from law enforcement, but also from everyone surrounding the criminal activity. Dewey (2016) similarly differentiated legitimate/illegitimate markets from illegal/legal ones, highlighting that some markets may be illegal according to the law, but considered legitimate by the population, thus

increasing the potential number of market participants compared to illegal and illegitimate markets.

When studying the size and influence of criminal organizations, Tremblay, Bouchard and Petit (2009) highlighted, as well, that where impunity is prevalent, criminal organizations tend to grow to wider territories as “criminal organizations tend to be large in settings where states are weak and opportunities abundant” (p.2). However, the authors’ argument centered around the idea that, by focusing on the small size of criminal organizations -in terms of direct members- researchers, law enforcement officials, and policy makers may miss an important aspect of the organizations’ reach, as discussed above.

Organizational reach may expand further given the rise of information technologies that are transforming all aspects of society. These technologies modify criminal commitment, making them more ephemeral and flexible (Goldsmith and Brewer, 2015). They also provide capacity (e.g., skills) and accessibility (e.g., potential collaborators) to criminal organizations involved in profit-driven activities (Leukfeldt et al., 2019). To provide insights on information technologies and criminal groups, the following section digs into the organization of profit-driven cybercrime.

2.1.3. On the Organization of Profit-Driven Cybercrime

Information technologies (ITs) can be considered as any technology “used to acquire, store, organize and process data as well as disseminate processed data which can be used in specified applications” (Rajaraman, 2018, p.17). Through new criminal opportunities, these technologies have influenced various forms of crime (Wall, 2007). For example, new types of crime have surfaced, like unauthorized access to computers (i.e., cybercrime) or mischief in relation to computer data. Other types of crimes have transformed: cheque fraud is (almost) a thing of the past, while online identity fraud is booming (Kemp, Llinares and Moneva, 2020; Anderson et al., 2019; Rege, 2009). The means have also evolved as, for instance, the possibility of doing online transactions has led to the rise of online drug marketplaces (Barratt, Ferris and Winstock, 2016; Christin, 2012; Décary-Hétu et al., 2012). All in all, as societies are developing and organizing around ITs, so are individuals behind criminal activities (Wall, 2007).

Usually, criminal activities related to the use of information technologies are known as “cybercrime”, and “profit-driven cybercrime” is cybercrime with a financial motive (as opposed to an ideological or political motive). Those behind cybercrime with profit motives are likely to form *organizations* or groups to orchestrate their activities (as opposed to lone wolves) (Broadhurst et al., 2014). Profit-driven cybercrime encompasses online economic crime, but also other types of crime, such as the sale of illegal drugs, as explained in the following section.

This section focuses on reviewing the literature on profit-driven cybercrime given that several studies have looked at how those behind profit-driven cybercrime organize (Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Kleemans and Stol, 2017a, b, c, d; Odinot et al., 2017; Bulanova-Hristova et al., 2016; Leukfeldt, 2014). The three main findings of these studies can be summarized as (1) online offender convergence settings play an important role, (2) the organization of those involved in profit-driven cybercrime is still locally embedded and (3) their structure is similar to that of traditional criminal groups. Each of these findings is discussed below.

Online Offender Convergence Settings

When studying profit-driven cybercrime, one can hardly ignore online meeting places where such criminal activities are discussed. Extant research has looked at how online meeting places are organized, focusing on open and closed forums and chat rooms as well as darknet markets (also known as cryptomarkets or anonymous online marketplaces). They are known as loose and flexible networks of individuals who sometimes associate for criminal purposes (Dupont et al., 2017; Dupont et al., 2016; Holt and Smirnova 2014; Yip, Webber and Shadbolt, 2013; Holt 2013; Motoyama et al. 2013; Décary-Hétu and Dupont 2012; Christin, 2012; Holt and Lampke 2010 and many more).

Leukfeldt, Kleemans and Stol (2017d) summarized well the function of these online places by using Felson’s (2006) offender convergence setting concept[5]. “Offender convergence settings” refers to physical places where individuals involved in criminal activities meet, such as bars, to ensure continuity and structures in their groups. These

[5] Soudijn and Zegers (2012) also employed the term in their paper *Cybercrime and virtual offender convergence settings*.

places also allow the recruiting of individuals outside of the criminal groups' direct network. In the traditional literature, offender convergence settings are important as social relationships are clustered and sometimes criminal groups need to find outsiders to complete their schemes (Kleemans, 2007); these settings provide a place for them to reach beyond their direct network.

Leukfeldt, Kleemans and Stol (2017d) posited that online meeting places, such as forums and chat rooms, represent *online offender convergence settings* that can be used for market (trading of products or services), social (discussing), or learning (sharing skills) purposes. Through them, criminal expertise can be sought, co-offenders can be found, various criminally related products can be bought and sold, and even new skills can be learned (Leukfeldt, Kleemans and Stol, 2017d). The sphere of economic influence of criminal groups who make use of them can expand significantly.

Research on the economic aspect of these settings have highlighted the industry that has developed, one that specializes in the production, distribution, and sale of illegal online products and services. This industry centers around specialization and professionalization (Thomas et al., 2015), increasing the productivity and profitability of the individuals involved (Lusthaus, 2018; Moore et al., 2009). Thus, one does not need to know the whole crime script of credit card fraud as one can just steal credit cards and sell them online to other users specialized in cashing out (Hutching and Holt, 2015). Through this industry, highly skilled individuals can specialize in one skill and outsource the remaining tasks (Van Wegberg et al., 2018).

Local Embeddedness

Although information technologies are borderless, most profit-driven cybercrime organizations are still locally embedded: individual context and social ties matter. Lusthaus and Varese (2021) and Lusthaus (2018) emphasized the offline and local dimension that characterize groups behind profit-driven cybercrime. Many studies also showed that online offender convergence settings do not necessarily play an important role in the growth and origin of criminal networks involved in profit-driven cybercrime (Leukfeldt et al., 2019; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a, b, c, d; Leukfeldt, 2014).

For example, Leukfeldt (2014) presented a case study of phishing in Amsterdam and found that the current literature provided an incomplete picture by focusing only on online settings. In the given case study, the author highlighted that group members knew each other from the physical world rather than through online interactions. Those engaged in the phishing scheme were found to be limited by their social opportunity structure (Kleemans and De Poot, 2008): the people they knew. They did not take advantage of large offender convergence settings where phishing schemes were discussed and orchestrated as reported in Soudijn and Zegers (2012). Considering these findings, Leukfeldt (2014) stressed the importance of identifying trends in the origin and growth of criminal organizations beyond online settings.

Leukfeldt, Kleemans and Stol (2017a,b) investigated criminal networks involved in online banking theft (phishing and malware) in The Netherlands, Germany, the United States and United Kingdom. They evaluated whether the networks studied grew due to social contacts (who you know, your connections through your everyday life) or forum interactions. By comparing social contacts with forum interactions, the authors developed four models of organizational growth: “(1) growth entirely through social contacts, (2) social contacts as a base and forums to recruit specialists, (3) forums as a base and social contacts to recruit local criminals and (4) growth entirely through forums” (Leukfeldt, Kleemans and Stol, 2017a, p.17). Findings illustrated that most of the networks studied fell into the first two models, suggesting that “offline” social contacts still play an important role in the formation, functioning and growth of criminal networks involved in profit-driven cybercrime.

Note that criminal groups that formed mainly via forum interactions (models 3 and 4) were less prevalent, but still existed. Leukfeldt, Kleemans and Stol (2017a,b,c) found evidence of these groups in criminal networks involved in online banking theft. These criminal networks formed flexible associations with members established in different countries. They were more likely to conduct high tech crimes (such as sophisticated malware to steal banking credentials) that do not require a high degree of victim/offender interactions (as opposed to phishing through phone calls).

Structure Similar to Traditional Criminal Organizations

To conceptualize the organization of profit-driven cybercrime, Leukfeldt, Lavorgna and Kleemans (2017) investigated whether criminal networks involved in online banking theft met the definitions of organized crime. The authors concluded that, given loose definitions of organized crime as more or less stable organizations with structured links among individuals, the networks studied held the minimum sets of characteristics necessary to be considered "organized crime". However, the authors highlighted that the cybercriminal networks studied were far from how organized crime is usually depicted, namely, as long-term hierarchical organizations with power in the economic and political spheres (see von Lampe (2008) for differences between conceptions and realities around "organized crime").

Instead, the structure of profit-driven cybercrime organizations resembles that of traditional criminal organizations: small and loosely organized (Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a, b, c, d; Leukfeldt, 2014). For example, Leukfeldt (2014), Leukfeldt, Kleemans and Stol (2017a,b,c) analyzed various networks involved in online banking theft and found that none of the networks studied had a strict hierarchical structure, yet they all had dependency relationships and functional roles. Through these studies, the authors illustrated that the majority of networks studied had three layers: **core members** who initiate and coordinate the attack, **enablers**[6] who provide services necessary for the crime script, and **money mules** who help hide financial trails.

When analyzing enablers, Leukfeldt, Kleemans and Stol (2017a, b, c) differentiated two types: professionals and recruited. **Professional enablers** provide professional services (usually criminal, such as writing malware) to all kind of criminal groups. **Recruited enablers**, on the other hand, are recruited by a criminal group for a specific service, such as a bank employee who can provide information on victims' accounts. Recruited enablers are usually involved with only one criminal network and are given a small fee for their service. Both types of enablers are recruited through social

[6] In Leukfeldt (2014) and Leukfeldt et al. (2020), individuals providing services to core members are called facilitators, rather than enablers, recalling the concept used in previous studies to talk about actors from the legal realm involved in criminal organizations (for a review, see Morselli and Giguère, 2006).

contacts or online offender convergence settings (Leukfeldt et al. 2020; Leukfeldt, Kleemans and Stol, 2017a, b, c; Leukfeldt, 2014).

Overall, most organizations involved in profit-driven cybercrime are locally embedded and their structures are similar to traditional criminal organizations (Leukfeldt et al., 2020; Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a, b, c; Leukfeldt, 2014). However, profit-driven cybercrime is a broad term that encompasses online economic crime. Why the concept of "online economic crime" is preferred in this thesis is explained below.

2.2. From Cybercrime to Online Economic Crime

Crime that leverages information technologies usually falls under the cybercrime umbrella. This section starts by briefly outlining the impracticalities of the concept that led me to avoid talking about cybercrime in general. Then, based on Naylor's (2003) profit-driven crime theory, how online economic crime is viewed and understood in this thesis is explained.

Cybercrime is a wide concept in criminology as most definitions of cybercrime refer to the use of "cyberspace" to "facilitate acts of crimes and deviance" (Holt and Bossler, 2014, p.21). In such a definition, cybercrime encompasses any kind of crime that uses technology, such as malware, cyberbullying, or online sexual exploitation of children. To make sense of this broad concept, several typologies have been developed, one of the most cited being Wall's (2007) typology, separating computer-integrity crime (e.g., cracking); computer-assisted crime (e.g., fraud, thefts); and computer-content crime (e.g., revenge porn). This typology, however, is limited as most crimes overlap in the categories. For example, ransomware is a type of malware that aims at compromising a device to encrypt its content. For the rightful owner to re-access the content, a ransom must be paid to the ransomware attacker. Such an attack can be interpreted both as a computer-integrity crime and as a computer-assisted crime. This example is one of many, making the typology often impractical.

Other researchers (such as Furnell (2003) and Smith, Grabosky and Urbas, 2004) have rather emphasized that "cybercrime" should be divided into two: (1) crimes that can happen only via the use of information technologies, such as cracking, and (2)

crimes that happen through technological means but could be performed through "traditional" ones as well, such as terrorism or bullying. To differentiate crimes involving technological means from traditional crimes in the second category, the "cyber" prefix is added. Terrorism becomes "cyberterrorism" and bullying becomes "cyberbullying" for example. However, as pointed out by Powell, Stratton and Cameron (2018), thinking with a dualist approach "terrestrial" vs "cyber" is problematic. It brings together crimes that may be totally unrelated in how they unfold and take place (e.g., terrorism and bullying). It also creates blind spots by forcing a focus on "cyber" instead of considering crime as a process taking place in a technology-embedded society (Powell, Stratton and Cameron, 2018).

Lusthaus (2018), on the other hand, argued that a better approach to classifying types of cybercrime (defined as acts of deviance happening online) is to focus on the main motivation behind the crime, such as political or financial. In his book *The Industry of Anonymity*, he focuses on "profit-driven cybercrime", which represents criminal activities that leverage information technologies for economic purposes. Such approach was also taken in several studies investigating cybercrime with financial purposes (Leukfeldt et al., 2020; Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a, b, c; Leukfeldt, 2014).

This conceptualization is narrower than the cybercrime concept but encompasses both predatory and market-based transactions, as defined by Naylor (2003). Naylor's (2003) conceptualization of profit-driven crimes was most fruitful in thinking about the types of crimes dealt with in this thesis. I develop on it further below.

2.2.1. Naylor's (2003) Conceptualization on Profit-Driven Crimes

Naylor's (2003) general theory of profit-driven crimes can be used to better conceptualize online economic crime and its specifics. Naylor (2003) argued that profit-driven crime can be better understood in economic rather than sociological terms. His typology considers the economic structures and consequences of profit-driven crimes, as well as the inherent characteristics of the underlying crime *script*.

The typology contains three types of profit-driven crime: predatory, market-based, and commercial. The first one, **predatory crime**, includes profit-driven crime that

involves illegal redistribution of existing wealth from one party to another and a readily identifiable victim, such as wallet theft. **Market-based crime**, on the other hand, involves profit-driven crimes that create new wealth (as opposed to transfers of wealth as with predatory crimes) and encompasses the production and/or distribution of goods or services that are illegal through *voluntary* transfers. Market-based crimes include, for example, the trade of illegal drugs or contraband products. The third category is defined as **commercial crime** and involves the illegal redistribution of legally earned income, such as embezzlement. Naylor (2003) mentions that, stereotypically (and thus not certainly), predatory crimes are more likely to be conducted by individuals, market-based crimes by groups and commercial crimes by corporations.

As the *crime script* behind profit-driven crime involves a complex series of interrelated activities and the degree of awareness of the individuals involved varies, Naylor (2003) differentiated between primary offences, which include predatory, market-based, and commercial offences, and secondary offences, which surround (or are a byproduct of) these crimes, such as corruption, violence, tax evasion or money laundering.

For example, based on Naylor's conceptualization, purse-theft is a primary offence that can be accompanied with violence – a secondary offence surrounding the primary one. Embezzlement, a primary offence, may require money laundering, a secondary one. Also, primary offences can be secondary offences in specific cases. For example, auto theft may be a primary crime, and the resale of the stolen car is a market-based offence that is secondary to the primary predatory offence. Such a script approach forces one to consider what the driving forces are behind a crime (such as theft or resale in the previous example).

Naylor (2003) added that, in general, predatory offences are characterized by violence, but rarely by corruption or tax evasion. On the other hand, market-based offences frequently involve money laundering and tax evasion and sometimes violence or corruption while commercial offences will rarely involve violence, sometimes money laundering or tax evasion, and frequently corruption.

This proposed general theory of profit-driven crimes was aimed at overcoming the vagueness around the conceptualization of profit-driven crimes (e.g., economic

crime or white-collar crime) as well as the technological fetishisms surrounding such crimes (e.g., *telemarketing* fraud or *internet* fraud), which, according to the author, create misleading and artificial distinctions. Naylor's (2003) conceptualization is helpful in defining the topic of this study: online economic crime, although Naylor would most likely criticize the use of "online" (technological fetishism) and "economic crime" (vagueness). His potential critiques are addressed below.

2.2.2. Defining and Differentiating Online Economic Crime

Online economic crimes are online predatory crimes: they encompass crime happening through information technologies that impose wealth redistributions with clear victims and perpetrators. However, the term "online economic crime" is favored over "online predatory crime" for two reasons. First, "predatory" refers to *predator* (a term often linked to animals in popular imaginaries) and implies the exploitation of others through violent means when necessary. Further, Naylor (2003) sees violence as the most probable secondary offence surrounding predatory profit-driven crimes. Online economic crime, on the other hand, focuses on stealing wealth through technological means, and rarely (if ever) induces physical violence. For these reasons, using the word "predatory" tends to inaccurately associate violence with the crime[7].

Second, the word "online" stresses that the economic crime studied takes place through information technologies, although no specific technology or type of crime is chosen. The term stresses that the "redistribution of wealth" must happen through information technologies, while other aspects surrounding the crime (such as money laundering) are not bound to the "online space".

By clearly defining *economic crime* as illegal wealth redistribution where there are victims and perpetrators, the vagueness trap of the term "economic crime" is avoided. By focusing on the *online* means of redistribution, fetishism over one technology is avoided, while a focus can be put on the new capabilities that information technologies enable.

[7] This argument does not dismiss the psychological violence that victims may experience due to the crime. The idea is to avoid imposing an impression of physical violence surrounding online economic crime.

In terms of new capabilities, information technologies contract time and space for specific human actions (e.g., buying products, surfing online) and interactions (e.g., online discussions). Such contraction increases the number of criminal opportunities, as offenders do not need to physically move to commit a crime and can target multiple victims at the same time (Llinares and Johnson, 2018; Leukfeldt and Yar, 2016; Yar, 2005). Information technologies also enable pseudo-anonymous interactions, which is believed to decrease offenders' fear of apprehension (Pittaro, 2007) while allowing individuals to endorse multiple personalities (Yar, 2005). Pseudo-anonymity is also believed to depersonalize victims for offenders (Montoyama et al., 2013).

However, why not use the mainstream label "cyber" to stress these capabilities? "Cyber" refers to the ***cyberspace metaphor*** and focuses on dichotomizing the world: the "cyberworld" and the physical world (Powell, Stratton and Cameron, 2018). Mumby and Spitzack (1983) explained how the use of metaphors can be problematic: it oversimplifies a problem and systematically imposes a focus on certain aspects while disregarding others. Their use may lead to metaphoric entrapment meaning that "the way in which a concept is understood becomes so tied up with a particular metaphoric structure that alternative ways of viewing that concept are obscured, or else appear to make less sense" (p. 166).

The *cyberspace* concept represents such a metaphorical entrapment, drawing the world in two distinct categories: an oversimplification that limits our conception of the world (Brown, 2006). More and more researchers are cautioning against the use of the cyberspace concept, arguing that it obscures the varying degrees in which information technologies are embedded in everyday life (Powell, Stratton and Cameron, 2018; Graham, 2013; Brown, 2006).

Moreover, in the past years, scholars in the field of crime and technology have moved past this metaphorical entrapment. Some have focused on studying the "geographies" behind crime and technology: what makes specific crimes related to technology cluster in specific regions of the world (Lusthaus and Varese, 2021; Lusthaus, Bruce, Phair, 2020). Others have focused on understanding how the embedded nature of technologies shape action and interaction in everyday life related to deviance (Powell, Stratton and Cameron, 2018). In the past five years, as opposed to studying the "cyber" aspect of the crime, a group of scholars have taken as a starting

point the individuals and their surrounding networks to understand the organization of profit-driven cybercrime (Leukfeldt et al., 2019; Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Kleemans and Stol a,b,c,d; Leukfeldt, 2014).

This study avoids the use of the term “cyber” to prevent drawing readers into a metaphorical entrapment. **Instead, this thesis investigates online economic crime, conceptualized as online illegal wealth distribution.** Naylor (2003) stressed that profit-driven crimes are better understood as a series of actions. This is highly relevant for online economic crime, as such crime usually requires **a series of actions, a scheme, to be successful.**

For purposes of clarity, Figure 1 defines cybercrime, profit-driven cybercrime, and online economic crime and provides examples for each type. It illustrates that cybercrime is a wide concept that encompasses pretty much every criminal activity happening through information technologies. Profit-driven cybercrime, on the other hand, focuses on “profit-driven” activities happening online, while encompassing both predatory and market-based profit-driven crime. Online economic crime focuses on illegal wealth distribution happening through online means, considering that such redistribution requires a series of actions. **The actions surrounding the distribution are not necessarily happening online; only the illegal wealth redistribution is**. Such conceptualization was helpful throughout the thesis. Hopefully, it can enlighten other scholars who wish to understand the dynamics behind crime and technology.

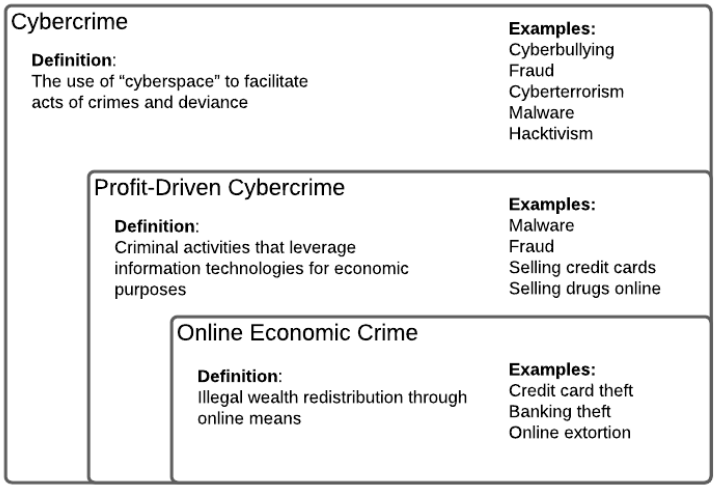

Figure 1 Concepts Linking Crime and Information Technologies

Online economic crime is generally more complex than traditional economic crime, like wallet theft, requiring a certain level of technical knowledge and skills. For example, a scheme behind online banking theft could require one to send phishing emails meant to induce a person to click on a malicious link. The malicious link, once clicked, could then compromise the victim's device and install a keylogger, a malicious software meant to record and exfiltrate everything that the victim types. The malicious actors, in this case, would be interested in the specific moment when the victim visits a banking website and enters their[8] credentials. Once stolen, the credentials would be used to connect to the victim's bank account and transfer money to a bank account controlled by the perpetrators. Another example is online extortion using ransomware, which is malicious software that compromises a device, encrypts the content, and asks for a ransom in exchange. A malicious group could scan the external perimeter of a corporate network to try to find vulnerabilities. If one is found and allows the group to infiltrate the corporate network, then a ransomware could be launched on the network to encrypt the content and a ransom would be asked to re-access the content.

Both examples involve a series of actions that result in a zero-sum game with a monetary goal, although the means to achieve the goal differ. Naylor's (2003) conceptualization is also helpful to identify the various secondary crimes involved in online economic crime. They may include, for example, market-based transactions to sell the stolen credit cards, money laundering to launder the stolen money, and, most importantly, many crimes related to unauthorized access to a computer and mischief in relation to computer data.

Legal Tasks and Online Economic Crime

Apart from secondary crimes involved in the series of interrelated tasks, the orchestration of the online economic crime often requires more coordination and mundane tasks that may resemble licit tasks, such as creating websites or maintaining an infrastructure of servers.

These mundane tasks have been reported by Collier et al. (2020), who interviewed individuals involved in booter services. Their finding stressed that a great number of tasks were outsourced to low-paid contractors, who do the "invisible" work

[8] "Their" is used to avoid gender-specific phrasing throughout the thesis.

that is or resembles legitimate work. Such work (in the case of this study sysadmin-like work) was reported to yield little profit while being boring (Collier et al., 2020).

Similarly, when studying networks involved in banking theft, Leukfeldt, Kleemans and Stol (2017a, b, c, d) mentioned core members recruiting enablers to build homemade phishing websites (programmers), write malware, or translate texts. Moreover, Leukfeldt et al. (2019) investigated how the availability and use of information technologies may change criminal cooperation. Their conclusions highlighted individuals with greater technical knowledge positioned at the periphery of the group, dubbed enablers. Their role should not be underestimated given that most members in the network studied did not have the required technical expertise to successfully achieve the crime.

Bijlenga and Kleemans (2018) found that some individuals and/or organizations with IT expertise were actively leveraged by criminal organizations. They studied five Dutch criminal investigations where expertise in the information and technology sector was sought by individuals involved in criminal activities. In three of the five cases, the basis of the collaborations was a legal business relationship. Such a relationship was possible because the criminal nature of the tasks was not always obvious; the good or service provided was legal, while its usage was not.

Hence, business collaborations can be established without the contractor or seller knowing that the product or service provided will be used for criminal means. As stated by Leukfeldt et al. (2020): “the criminal character does not have to be clearly visible to the person concerned or it can be denied afterward” (p.6). In this sense, the neutrality of IT-related tasks creates a grey area that can be leveraged to successfully orchestrate criminal activities (Leukfeldt et al., 2020; Bijlenga and Kleemans, 2018)

2.3. Informal Economies

Collier et al. (2020), Leukfeldt et al. (2019), Leukfeldt, Kleemans and Stol (2017a, b, c, d) and Bijlenga and Kleemans (2018) found that individuals with IT skills end up conducting activities for criminal groups. This **grey area** reminds of informal labor markets where workers wade between legality, illegality, and criminality. The section below reviews what is known on informal markets and their online counterpart. It

provides useful insights on the reality of informal workers, one that can be used to better understand workers with IT expertise who end up involved in online economic crime.

The “informal economy” is a broad and multifaceted concept tackled by scholars from various disciplines, including economics, sociology, and criminology. In general, informal economies are associated with the reverse side of the official economy: the unregulated or unregistered economic activities (Ponsaers, Shapland and Williams, 2008). For this thesis, informal economic activities are economic activities that escape normal record keeping (Ojo, Nwankwo and Gbadamosi, 2013), thus representing “all income-earning activities that are not regulated by the state in social environments where similar activities are regulated” (Castel and Portes, 1989, p.23). In such markets, the product or the service exchanged is not necessarily illegal; it is rather the means by which it is produced and distributed that is illegal. These markets are known to be volatile and flexible, but also inherently unstable (Vande Walle, 2008), and their existence is not necessarily linked to poverty: their form depends on the context and the goal of the participants operating in them (Vande Waller, 2008; Castells and Portes, 1989).

Formal and informal economies have a symbiotic relationship (Harding and Jenkins, 1989) and decisions in one may change actions in the other. For example, strong state control should diminish the size of an informal economy, but it may also provide new potential profitable opportunities to individuals who would be willing to bypass the controls (Portes and Haller, 2010). Portes and Haller (2010) defined three aims of informal economies for market participants: survival, dependent exploitation (such as decreased labor costs), and growth (such as capital accumulation through greater flexibility) (p.405-6). Thus, considering the latter, informal economies are not always destructive: they can provide jobs to otherwise unemployed individuals, lower costs for products and services and foster innovation (Ojo, Nwankwo and Gbadamosi, 2013; Portes and Haller, 2010). Informal economies are also highly dependent on social ties to develop trust among market participants (Portes and Haller, 2010; Shaplan, 2004). Their inception and development are highly reliant on the social structures behind them as well as their geographical position, such as access to trade routes or labor (Shaplan, 2004). Their economic activities, although informal, are also often considered socially acceptable by their enclaves. Informal workers engage in informal markets due

to autonomy, social networks, ease of entry, flexibility, and freedom (Ojo, Nwankwo and Gbadamosi, 2013).

However, due to their informal status, these markets may benefit groups involved in criminal activities. For example, informal financial markets represent attractive settings for money laundering (Vande Walle, 2008). Hagedorn (2007) also found that US gangs played *protection* roles in informal businesses to replace the legal instruments usually accessible in the legal realm. However, Sabet (2015) studied how informal and criminal sectors overlap in Mexico and argued that the extent to which criminal groups can penetrate informal economies to mitigate the opportunity costs (i.e., for protection purposes) depends on 1) the degree of illegality and legitimacy of the product traded and 2) how market participants overcome the transaction risks and the threat of law enforcement. Sabet (2015) highlighted, that, in theory, informal settings offer opportunities for criminal groups to mitigate transaction failures by providing, for example, credit, insurance, or protection, but, in practice, informal workers tend to solve these costs through clientelism (exchanging goods and services for political support in favor of tolerating their activities) or self-help associations - associations that provide support to individuals who share a common experience (p.2).

Nevertheless, even if informal workers tend to avoid mingling with criminal groups to mitigate uncertain transaction costs, informal markets do create an environment that benefits criminal activities in many ways, such as corrupting officials, reselling counterfeit or stolen goods or purchasing unlicensed cars. (Sabet, 2015; Shaplan, 2004). Moreover, Ojo, Nwankwo and Gbadamosi (2013) studied 30 informal entrepreneurs in the UK and found that these informal entrepreneurs seized opportunities in criminal spheres. Thus, the line between informal and criminal markets is often difficult to draw in practice, as these markets merge and are interrelated in various ways (McElwee, Smith, and Somerville, 2011; Vande Walle, 2008; Shapland, 2004).

Online Informal Economies

Nowadays, the internet has become a robust channel for economic transactions (Cambini et al., 2011). Given the difficulties legal institutions globally have had in regulating online economic transactions (Murray, 2007), **online informal economies have been thriving** (Rangaswamy, 2019; Dobson et al., 2015;). Moreover, online

informal economies do not necessarily need social embeddedness to properly function (Granovetter, 1985): the potential trust problems and uncertainties that market participants face have been partially neutralized with the rise of informal institutions (Dobson et al., 2015; Kshetri, 2010). Informal institutions are platforms providing mechanisms for neutralizing trust issues among market participants through various reputation systems, such as providing feedback.

Of interest to this thesis are informal institutions known as digital labor platforms, which gather a pool of IT workers who could be recruited by online economic crime organizations. The next section reviews what is known on the internal dynamics of these platforms.

2.3.2. Digital Labor Platforms

There exist various informal institutions (e.g., eBay or Amazon), and those of interest to this thesis are digital labor platforms (e.g., Freelancer.com, Upwork, Fiverr), which offer a matching service linking demand for labor with its supply (Drahokoupil and Piasna, 2017). Their rise and expansion, in the past years, have led to a reconfiguration of employer-employee relationships, minimizing outside regulations of employment and evading company-like structures of employment (Lehdonvirta, 2016). Labor contracts happening on these platforms are consequently far away from *standard employment relationships* (SER), which are characterized by full-time, permanent, and direct employment by a company (Strauss, 2018a). They rather foster flexible, yet also challenging, working conditions, as explained below.

In short, digital labor platforms are assumed to foster market-like dynamics in the supply of and demand for labor, thus reducing hiring transaction costs. They also expand the labor supply by lowering barriers to entry to the labor market (Drahokoupil and Piasna, 2017). Drahokoupil and Fabo (2016) outlined that these platforms have *three* interesting features: they provide an algorithm to focus on effective matching, they reduce hiring transaction costs, and they provide services, through reputation and monitoring systems, that reduce the risks involved in market transactions. They are assumed to be efficient and flexible at mediating clients (labor demand) and independent contractors (labor supply). Through them, a contingent workforce is available on demand

and can be dismissed as soon as a task for which the worker is hired is completed (Schmidt, 2017).

However, with direct access to workers from low-income countries, global labor arbitrage takes place on these platforms: jobs move to low-cost labor markets, consequently leading to competition and reduced wages (Roach, 2004; Drahokoupil and Piasna, 2017). These platforms thus reduce workers' rights and working conditions while driving wages to the floor (Schmidt, 2017; Drahokoupil and Piasna, 2017; Drahokoupil and Fabo, 2016).

Also, the easiness in hiring individuals has led to a high prevalence of micro-tasking: dividing the contracted work to the point that the independent contractors are unaware of the final product (Schmidt, 2017; Drahokoupil and Piasna, 2017). Such micro-tasking is believed to be negative for workers as it removes their control over the work process as well as the reward felt when seeing the final product (Drahokoupil and Piasna, 2017).

Moreover, not only is the price (wage) low, but it also usually covers only the marginal costs, ignoring additional long-run costs such as acquiring new skills (Malhotra and Van Alstyne, 2014, p. 25). However, Graham, Hjorth and Lehdonvirta (2016) pointed out that the positive and negative aspects of these platforms depend on the geographic locations in which workers are. For example, some workers may enhance their working conditions when established in parts of the world where unemployment is high. Others, on the other hand, might be forced to accept low-wage contracts, leading to *precarious*[9] working relationships.

Cloud Work on Digital Labor Platforms

To unravel the type of work offered on digital labor platforms, Schmidt (2017) offered an interesting taxonomy: cloud work, crowd work and gig work. Cloud work refers to work that can be done remotely via the internet. Crowd work, on the other hand, involves tasks that cannot be completed by a single individual but only with an undefined group of people (e.g., photo tagging, product categorization). Lastly, gig work refers to tasks that need to be done in a specific location and time (e.g., Uber drivers). To

[9] For a review on the concept of *work precariousness*, see Strauss (2018b).

differentiate the platforms offering such work, Schmidt (2017) stated that web-based digital labor encompasses both cloud work and crowd work while location-based digital labor involves accommodation, transportation, delivery services, household services and personal services (p.22).

Freelancer platforms are digital labor platforms that allow hiring an independent contractor based on their skills and knowledge, thus hiring *cloud work* (Schmidt, 2017). Payments are usually negotiated individually, and the jobs contracted via freelancer platforms are typically complex and specialized (as opposed to automated crowd work), including SEO optimization, software and website development, marketing design, writing and legal writing (Schmidt, 2017, p.14). These platforms are thriving, as, according to the Statista Research, about 59 million individuals were freelancing just in the United States in 2020 (Statista Research Department, 2021).

Labor market transactions taking place specifically on freelancer platforms are not as frictionless and flexible as argued by their proponents. There are still global frictions as labor demand clients are more likely to select workers who are culturally close to them, especially in terms of language (Hong and Pavlou, 2013; Gefen and Carmel, 2008). Also, Lustig et al. (2020) interviewed full-time employees who hired freelancers as part of their job responsibilities and identified two additional transaction costs. The first transaction cost referred to a task definition problem: “the act of carving out a piece of one’s work, describing it in a job description, defining the milestones, setting the pay rate, and putting it on a freelance platform” (Lustig et al., 2020, p.16). Often, the tasks were not well defined, which resulted in misunderstandings with the freelancer. The second transaction cost was related to managing freelancers, which was time consuming as well as sometimes difficult as some freelancers tend to not abide by a company’s worker compliance guideline.

Informality, Criminality and Digital Labor Platforms

The difficulties in regulating digital labor platforms have been highlighted by several scholars (Schmidt, 2017; Drahokoupil and Fabo, 2016; Drahokoupil and Piasna, 2017; Strauss 2018a). Transacting parties are in different geographic regions, which often blurs under which regulation or national standard the work falls (Schmidt, 2017). Additionally, the burden is on independent contractors (rather than employers) as “self-employed” individuals to declare their activities and take care of their social security

contributions. Thus, most of the informal work is neither taxed nor covered by social insurances (Drahokoupil and Piasna, 2017, p.337). Such a lack of regulations and minimum standards increase competition among labor supplies and puts downward pressures on pay and working conditions (Drahokoupil and Piasna, 2017, p.336). These platforms become tools to circumvent national laws for “consumer protection, workers’ rights, minimum wage regulations and social security contributions” (Schmidt, 2017, p.2). In the end, these informal platforms represent modern online informal economies.

These online informal economies, just like the offline counterparts, may create an environment that is auspicious for criminal activities. So far, two freelancer platforms have been associated with criminal online activities. Farooqi et al. (2017) tagged the platform SEOClerk as a “blackhat marketplace” and Garg, Camp and Kanich (2013) considered the platform Freelancer as a hub for criminal activities. The latter assumption was based on the results of Motoyama et al. (2013), a study that investigated the on-demand platform Freelancer and concluded that 66% of the jobs posted were legitimate, meaning that about 33% of the remaining tasks were likely related to illegal activities, included thwarting security mechanisms, or sending spam.

Additionally, these platforms gather informal workers with an IT expertise that can be of interest to those involved in online economic crime (Collier et al., 2020; Leukfeldt et al., 2019; Leukfeldt, Kleemans and Stol, 2017a, b, c, d; Bijlenga and Kleemans, 2018). When investigating five case studies where individuals or organizations with IT expertise were sought by criminal organizations, Bijlenga and Kleemans (2018) concluded that the business relationships were quickly directed at criminal collaborations. In “traditional” informal markets, workers were found to avoid criminal ties when possible (Sabet, 2015) while also accept economic opportunities in the criminal sphere when the potential returns were good (Ojo, Nwankwo and Gbadamosi, 2013).

This raises the question: to what extent the informal IT workforce available on digital labor platforms can be considered “available” for those behind online economic crime? To unpack this informal/criminal relationship, this thesis needs to conceptualize what is meant by being willing to participate in criminal activities. To do so, Matza’s (1990) work on “drift” is presented, followed by Goldsmith and Brewer’s (2015) digital drift concept.

2.4. The Uncertain State: Drifting

What makes an individual willing to participate in crime? Matza (1990) visited such a question in his seminal book *Delinquency and Drift,* which widely contributed to understanding crime and delinquency in the field of criminology (Blomberg et al., 2018). He suggested that, rather than conceptualizing delinquency as criminal actors who continuously break the law, delinquency should be considered as a transient and temporary legal status that individuals intermittently embody. Thus, most delinquents will play intermittently delinquent and conventional roles, and, for most of their lives, they will stay on the conventional side and not offend (Matza, 1990). When they do, they will first drift. The "drifting" concept is what is of interest to this study. The concept has been developed for juveniles rather than individuals involved in online economic crime, yet it provides nuances and understanding as to why and how an individual may end up in a state where criminal activity is possible. I first present a review of Matza's main thesis to understand the background context in which the drifting concept was developed.

That delinquency should be considered as a transient and temporary legal status that individuals intermittently embody is oppositional to sociological theories of deviance (Miller, 2017 [1958]; Cohen, 1958 and Cloward and Ohlin, 2013 [1960]), which posit that delinquent subculture embraces norms and values that support criminal activity. Matza (1990) rejected the idea that delinquents are fully committed to a delinquency subculture. The author rather argued that there exists a *subculture of delinquency* (as opposed to a delinquency subculture). This subculture of delinquency is a setting in which the commission of criminal activity is acknowledged and is the outcome of delinquent values, norms, and sentiments. However, this subculture is not "fully committed to crime", given that delinquents *apprehend* the potential legal consequences of their acts and rationalize them through conventional norms. Indeed, as highlighted by Matza (1990), once a criminal act is committed, delinquents rationalize the said act through neutralization techniques that approximate conventional norms. These techniques are similar to conventional excuses, such as negating an offense (e.g., self defense, accident, or insanity), having a sense of injustice (e.g., perceived inconsistency of individualized justice), assertion of tort (e.g., negation of victims) and the primacy of customs (e.g., consensual crimes). If they were fully committed, such apprehension and rationalization would not take place. These neutralization techniques have been revisited

in Sykes and Matza (2017) as: 1) denial of responsibility; 2) denial of injury; 3) denial of victim; 4) condemnation of the condemners, and 5) appeal of higher loyalties.

Delinquents are thus committed to neither delinquent nor conventional norms; they rather exist in a limbo between these two spaces. The drift (which is of interest to this thesis) represents this movement between conventional and criminal actions. Matza (1990) defines “drift” as the episodic moments of release from moral restraints: when the tie binding self to legal expectations is broken. Drifting does not guarantee a criminal act; it only makes the criminal act possible or permissible by temporarily removing moral restraints. The idea is to convey an image of individuals who “drift” in and out of these restraints yet embody the conventional “restrained” role most of the time. Matza (1990) also argued that the moral vacuum is not sufficient to explain the thrust that leads to criminal action and suggested that the missing element that pushes an individual into the criminal act is conceptualized as *will*. Two conditions -that can only happen once drift is realized- may activate such will: preparation and desperation. Preparation refers to the process of learning from experience (personal or from others) that a criminal act is a feasible behavior that is relatively easy to do; it implies the *will* to repeat infractions.

Desperation refers to a loss of control over one’s environment, leading to the commission of crime to re-establish the order; it implies the *will* to commit new infractions. The *will* represents the thrust for potential for criminal action implicit in drift (p.191). However, it is not automatic: it can be deterred through various processes, such as the presence of a guardian (Cohen and Felson, 1979).

Overall, Matza’s (1990) work has been a source of development and inspiration in the field of criminology, shedding light on the processes behind delinquency and inspiring various studies on the matter (for a review, see Bloomberg et al., 2018). This understanding, along with additional work (see Piquero, 2004; Laub and Sampson, 2003; Nagin and Land, 1993) has led to the development of the concept of *intermittency* in criminal careers, which involves temporary abstinence from criminal activities followed by resumption of criminal activities throughout an individual’s criminal career (Piquero, 2004). Most delinquents follow zigzag paths, cycles of offending and non-offending (Laub and Sampson, 2003), which depends on various individual circumstances, including criminal achievements and potential sanctions (Ouellet, 2018).

2.4.1. Digital Drift

Although Matza's work focused on juveniles, it provides powerful theoretical concepts to assess how and why individuals may participate in criminal activities. Information technologies have changed the structure and scope of criminal activities and Matza's (1990) drifting concept has been used to grasp online criminal commitment processes (Holt, Brewer and Goldsmith, 2018; Goldsmith and Brewer, 2015).

Goldsmith and Brewer (2015) explored how the internet is changing how crime is organized and committed in their paper: *Digital Drift and the Criminal Interaction Order*. They argue that internet-related uses have fundamentally reconfigured the arrangements for criminal commitments in three ways: 1) lowering the bonding power of groups; 2) expanding the range of interactions possible for an individual; and 3) giving the power to individuals to decide when, how, and whether they want to affiliate with others (p.113).

According to the authors, the internet significantly reshapes criminal commitments by facilitating the encounter of individuals across time and space; in other words, it has increased networking opportunities. Technical affordances of the internet, such as the possibility to create (and amend) false identities (avatars) or the possibility to anonymously consume information, also encourage the fluidity and play of online encounters. Committing to a criminal group in an online environment represents a different type of commitment than committing to groups formed through face-to-face interactions as online encounters are characterized by movement, unpredictability and "absence of involvement".

Such a nomadic state allows individuals to engage and dis-engage in criminal activities more easily. To grasp such commitment patterns, Goldsmith and Brewer (2015) introduced the concept of *digital drift,* which is derived from Matza (1990). As defined by the authors, digital drift captures the ability of individuals to negotiate the engagement boundary in criminal commitment and emphasizes the idea that "drift into and out of criminal pathways can often be accidental or unpredictable" (p.113). Digital drift thus refers to the individual's episodic involvement in illegal actions, which takes place through the dynamic engagement between the features of the internet and the use made of them by individuals.

The internet also acts as a source of ideas and information, offering conditions for individual empowerment, allowing individuals to commit crime "more autonomously through facilitating self-instruction" (p.112). These conditions offer more choice and control to individuals on when and how to engage with others online. Goldsmith and Brewer (2015) concluded that the internet is a source and a facilitator of criminal interactions and stressed the need to develop a "criminal interaction order[10]" that incorporates these new *means* of social encounters (e.g., social networks, forums) and these new ways to gain criminal capabilities (i.e., social and criminal capital). They argued that such an approach could yield further insights on the processes behind digital drifts in and out of criminal commitments.

The digital drift concept stresses the ephemerality of criminal encounters happening in online environments, as well as the possibility for individuals to easily engage and disengage in criminal activities at their will. This conceptualization will be useful in the thesis when assessing the informal workers' dance and their potential ease at drifting in and out of crime-oriented spaces.

[10] Refers to Goffman's (1983) *interaction order*: the study of strategies and interaction rituals among individuals.

Chapter 3.

Thesis Objectives and Research Questions

Online economic crime involves a series of actions that aim at illegal redistribution of wealth through online means. The literature review above illustrated what is known on the organization of criminal groups (and groups behind profit-driven cybercrime) as well as factors influencing their growth. A few studies also highlighted the involvement of informal workers from the IT sector in the organization of online economic crime, a concerning finding considering that digital labor platforms (specialized in such fields) are thriving. However, what these workers represent for online economic crime organizations and these workers' impact on the reach and sophistication of the crime has yet to be researched thoroughly. Such an assessment may yield insights on various avenues to deter and prevent such crime by motivated offenders, but also by informal IT workers involved at the periphery of the crime script.

Specifically, this thesis uncovers contexts, motivations, and organizations of those behind online economic crime. While doing so, it assesses the role and availability of an informal workforce surrounding the crime organization and its likelihood to participate in such criminal schemes. This mixed-method thesis is divided in two parts, representing two objectives and four analyses.

The first part follows a qualitative approach, driven by the objective (**Obj. 1**): **To uncover the contexts and motivations that may drive individuals to participate in online economic crime**. This objective is achieved through two research questions related to two qualitative data sources. The first research question is (**RQ1**):

"What are the contextual factors and perceived motivations behind online economic crime?"

To answer this research question, 21 semi-structured interviews with experts knowledgeable about online economic crime are conducted. Experts' narratives are studied through an inductive thematic analysis[11].

The second data source is a chat log containing private conversations among individuals involved in online economic crime. To stay as close as possible to their conversations, the research question for this analysis focuses on finding their challenges and motivations, as opposed to contextual factors. Consequently, the research question is (**RQ2**):

"What are the main motivations and challenges behind those involved in online economic crime?"

This question is answered through an inductive thematic analysis of the conversations. Focusing on the challenges led to uncovering their context. The results of these two qualitative analyses emphasize the role of informal workers involved in various tasks related to online economic crime. The private chat log conversations led to uncovering a digital labor platform for IT-related products and services. The second part of this thesis studies the individuals interacting in the digital labor platform.

Throughout this thesis, individuals discussing on this platform are conceptualized as **informal IT workers** and the platform as an **informal platform**. Information about these informal IT workers was gathered thanks to an academic access to the Flare Systems[12] database, which is a private company monitoring various online spaces.

The second part of the thesis focuses on understanding this workforce's relationship between informal and criminal spaces. Since workers could not be interviewed, this is done through proxy analysis evaluating informal workers' commenting patterns between the informal platform and crime-oriented ones. Crime-

[11] Since I defined online economic crime as profit-driven, it may seem tautological to investigate the motivations behind such crime. A first iteration of the research question was "…motivation of those exploiting information technologies" instead of "online economic crime". The concept of online economic crime emerged from the interviews thanks to the inductive approach, leading me to reconsider the central topic of this thesis. Then, additional perceived motivations were found, along with interesting insights related to the financial reality of these individuals.

[12] https://flare.systems/

oriented platforms are platforms that take a clear criminal ethos in their branding, such as carding or money laundering.

To differentiate workers who talked on crime-oriented platforms, the concept of **drifter** is developed. It builds on Matza's drift (1990), which refers to episodic moments of release of moral restraints. Drifters are individuals from the informal workforce that end up discussing, at least once, in a crime-oriented space. When drifters discuss on crime-oriented platforms, they take action in the space, which is different from lurking or simply reading on these spaces. Commenting, however, is not criminal; it is only a step that illustrates that those individuals have drifted. In the drifting state, criminal activities are possible, yet not inevitable.

In this second part, a quantitative approach is taken, driven by the objective **(Obj. 2): To assess drifters' relationship between informal and crime-oriented spaces**. Two quantitative analyses are computed, each of them led by a specific research question. The first quantitative analysis aims at assessing whether drifters formed a distinct group that could be identified on the informal platform. If yes, then the drifters' distinctive group (and how it uses the informal platform) would require further investigation. The research question is (**RQ3**):

"Does drifters' behavior on the platform differ from that of non-drifters?"

A series of non-parametric Mann-Whitney U tests are conducted on drifters and non-drifters, based on behavioral indicators. Behavioral indicators reflect individual behavior on the informal platform, such as types of topics discussed and activity rate. To assess drifters' relationship between the informal space and crime-oriented ones further, the second quantitative analysis is longitudinal. It focuses on understanding drifters' commenting behavior on these spaces through time. The research question is (**RQ4**):

"How do drifters use the informal space compared to crime-oriented spaces over time?"

A group-based trajectory model is built, comparing drifters' commenting behavior between the informal space and crime-oriented ones over a nine-year period. Overall, the results of these four analyses shed light on contexts, perceived motivations, and organization of individuals involved in online economic crime. They also provide an

assessment of the role of informal workers at the periphery, and their likelihood to participate in criminal activities.

For clarity purposes, Figure 2 provides an overview of the thesis workflow, including the two research objectives, four research questions, four data sources, and four data analyses. Hopefully, through this summary, readers can grasp the topics of the upcoming chapters easily. Also, note that, given the mixed-method approach and the plurality of datasets, the simplest and most efficient way to present the thesis core is by presenting the methods and data followed by the results respectively for each analysis. This approach allows the reader to follow the methodological decisions and their impacts on the results. Figure 2 also shows which chapters cover which analysis. For one analysis, the first chapter contains the methods and data, and the second chapter contains the results.

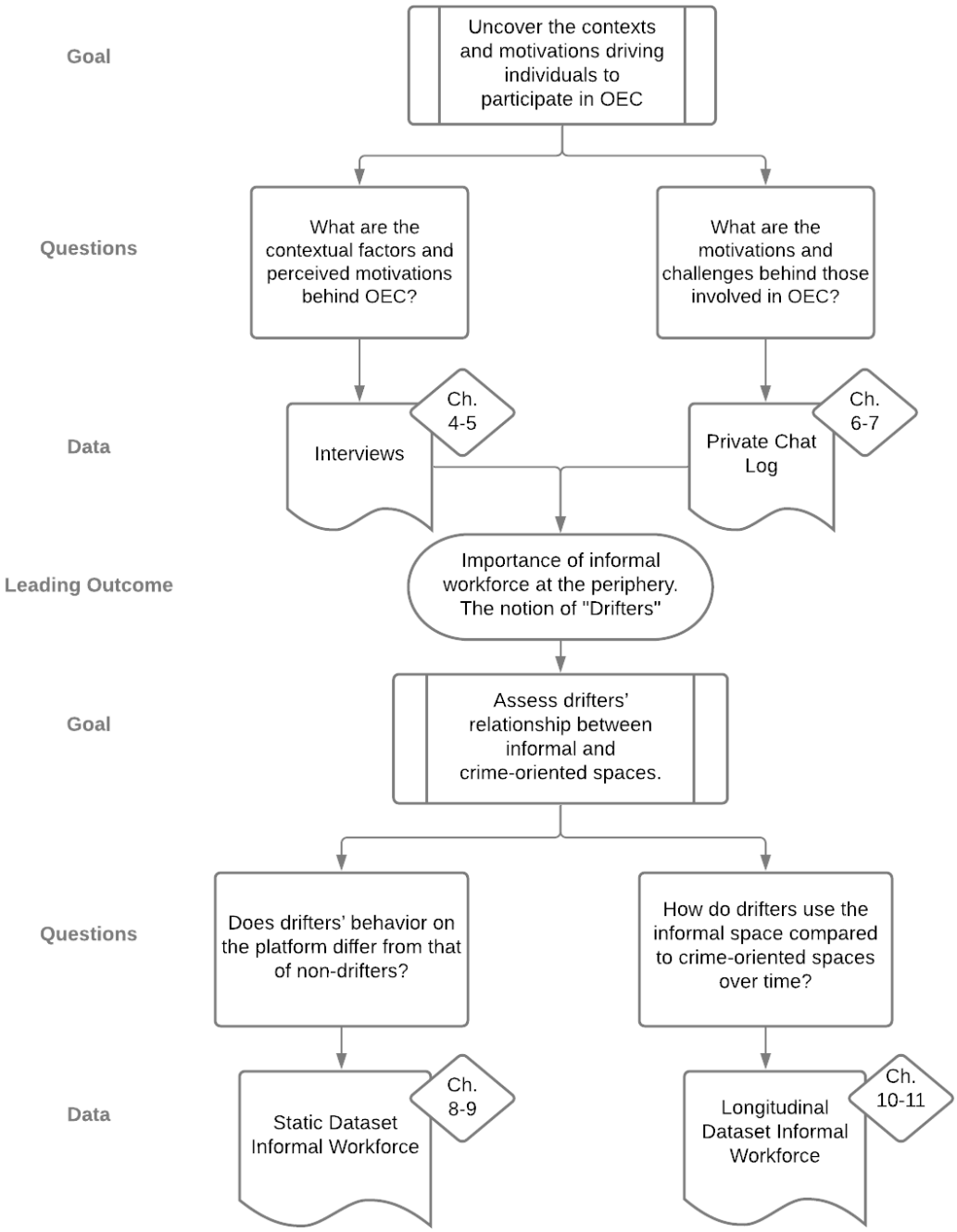

Figure 2 Thesis Workflow

(OEC stands for online economic crime.)

Chapter 4. **Methods for Interviews with Experts**

The first objective of this thesis is to uncover various contexts and motivations that may drive individuals to participate in online economic crime. To do so, semi-structured interviews were conducted with experts, driven by the question: *"What are the contextual factors and perceived motivations behind online economic crime?"* The following chapter presents the methodological steps followed to recruit and interview experts. Then the analytical strategy is outlined followed by ethical considerations.

4.1. Collaboration with the Stratosphere Laboratory

The interviews were conducted in close collaboration with the Stratosphere Laboratory. The Laboratory is part of the "Artificial Intelligence Centre at the Czech Technical University in Prague and works at the intersection of cybersecurity, machine learning, and helping others" (Stratosphere, 2021). Three members of the Stratosphere Laboratory actively collaborated in the research: Sebastian Garcia (assistant professor at CTU and director of Stratosphere Laboratory), Maria José Erquiaga (team leader of the aposemat project, part of the Stratosphere Laboratory) and Veronica Valeros (technical leader at Stratosphere Laboratory). They helped with participants' recruitment, interviews, and analyses. Their motives to participate in the research were the same as mine: to better understand the context and motivations of those behind online economic crime.

4.2. Recruiting Experts

The Stratosphere Laboratory is formed of well-established researchers from academia and the industry with an expertise in cybersecurity and cybercrime. The members have presented at international conferences where they have developed a network of professionals from all over the world. For recruitment, the Laboratory's international social network was leveraged. Members of the Laboratory were told about the study's aim: that I sought experts knowledgeable on the contexts and motivations that influence those behind online economic crime. However, no definition of who qualifies as an expert and who does not was provided. I relied on members' subjective

understanding of their network and who would be suitable for the study. The following section explains the rationale behind this approach.

4.2.1. Participants as Experts

The issue of what constitutes experts and expertise, as well as the extent to which “expert” knowledge is more valuable than the knowledge of other people, is a highly debated issue in social science (Bogner, Littig and Menz, 2009). There have been many attempts at defining who can be considered an expert (Baker, Lovell, and Harris, 2006), with criteria ranging from an individual’s position and knowledge, to how someone is publicly acknowledged or recommended by others (Moseley and Mead, 2001). Yet, there are no agreed-upon definitions (Baker, Lovell, and Harris, 2006) as the concept of “expertise” is a construct; there are no deterministic ways to specify who is an expert and who is not. The dangers of relying on experts’ knowledge for social science studies lie in assuming that experts’ knowledge provides the objective truth about a social phenomenon. Such a preconception can lead to research findings and subsequent policies based on deterministic assumptions (Bogner, Littig and Menz, 2009,). On the other hand, individuals with substantial knowledge on a topic can provide valuable insights on complex social processes and interviews with them can lead to interesting research orientations (Bogner and Menz, 2009). In the end, it is the responsibility of the researcher to choose who is an expert and defend that choice (Baker, Lovell, and Harris, 2006) as well as nuance the findings based on the limits of the established criteria.

Considering the field of cybersecurity and cybercrime, fixing a strict criterion to determine who is an expert and who is not can be problematic, given that skills and expertise range from low-level reverse engineering expertise to finding malicious activity in network traffic to investigating criminal groups in underground forums. Some could argue that the number of years active in the field would be an adequate “objective” criterion. Yet the field is evolving so quickly that those with several years of experience are often not up to date anymore on new emerging threats, as they move to management positions. My experience in the field has taught me that, in cybersecurity, expertise is not so much about status or position but more about interest and curiosity.

Another way of identifying experts is whether they are vetted by others in the field as such (Moseley and Mead, 2001). Such a criterion means that individuals

knowledgeable in a field can refer someone they consider a suitable expert for the study. Such a criterion considers referrers' assessments of who is an expert on the topic resulting from their experiences and interactions in the field.

The following criterion was the primary one used to accept a study participant: someone vetted by Stratosphere Laboratory members or other research participants as experts on the study topic. The referrers and research participants were aware of the study's first objective and referred individuals based on their own experiences and interactions in the field of cybersecurity and cybercrime.

However, to avoid presenting the narratives found as objective truth, which is the biggest identified danger of using the *expert* concept in qualitative research (Bogner, Littig and Menz, 2009), I stress throughout the results that the findings are associated with experts' understanding of the phenomenon, not necessarily an objective truth.

4.2.2. Recruiting Process

Throughout the recruiting process, Stratosphere Laboratory members actively helped finding research participants, contacting individuals in their network they thought would be knowledgeable on the study topic. When a contact accepted, an introductory email was sent and, through a series of online exchanges, a time and date was set for the interview and the consent form was shared. Additional participants were also recruited via a snowballing method: at the end of each interview, interviewees were asked if they knew other experts who would be knowledgeable on the matter. If so, participants contacted them first; if the response was positive, the new potential participant was contacted, and the same process mentioned above ensued.

This resulted in 21 interviews and 22 research participants, as one interview was conducted with two participants at the same time. The interviews happened between July and December 2020 and spanned from 40 to 180 minutes each, with an average of 90 minutes. In 19 interviews out of 21, Stratosphere collaborators came to the interview and sometimes asked questions to research participants. Their presence often made the atmosphere more friendly and comfortable.

All interviews happened online through Zoom or Jitsi, depending on the participant's preference. If research participants accepted, the audio was recorded using

the Otter AI software[13]. Each interview was transcribed and anonymized with an internal ID number. The recordings are kept in an encrypted external drive at the Stratosphere Laboratory office and protected by a password.

4.3. Interview Process and Consent Form

The interviews were semi-directed, and the interview process encompassed three topics. The first topic asked about experts' experiences at fighting cybersecurity threats and finding those behind the threats, the "attackers". This topic aimed at gathering hands-on experiences, but also led to discussing what experts thought motivated those behind the activity. It also brought interesting stories on individuals participating in online economic crime and how they organized. The second topic asked about contexts wherein those behind such activity cluster, and the third topic inquired about specific contextual factors that experts thought could influence individuals to participate in such activities. These three topics uncovered various contexts and perceived motivations that may drive individuals to participate in online economic crime (objective 1).

However, after the first five interviews, we (the research collaborators and I) quickly noticed that moving away from the formal interviewer-interviewee positions yielded a more relaxed atmosphere. Rather than asking predefined questions from the interview protocol, I semi-directed a discussion. Given the online setting in which the interviews took place and the sensitivity of the topics discussed, this change of *footing*[14] was important and subsequently, more meaningful information was shared. The remainder of the interviews started with a first question: "*Have you ever worked on specific cases of online economic crime, and you ended up finding the people behind them?*" Then, once participants started to share their experience and knowledge on the topic, I semi-directed them by making further inquiries based on the protocol's topics and their narratives. Such an approach made sense because participants had read the

[13] https://otter.ai/

[14] Footing is a concept developed in Goffman (1981, 1974) that refers to the projected self. When I moved away from the interviewer position my projected self changed from a strict interviewer to an interested party. This transformed the participation framework in which the interview took place.

consent form and were aware of our research objectives, so they could share their knowledge within the frame and structure that they preferred.

The consent form sent to research participants is available in Appendix A. It includes a thesis summary that was submitted 12 months prior to the final writing of the thesis. The prior summary focused on understanding the contextual factors and motivation of individuals exploiting information technology opportunities. As an example, individuals involved in distributing banking trojan applications related to a botnet (known as Geost (Garcia et al., 2019) was mentioned. Since then, the thesis summary has changed because of the additional qualitative analysis and the subsequent two quantitative sections that were added post-interviews, all focusing on online economic crime. However, regardless of these changes, the specific objective to which research participants agreed to contribute is the same: to understand the contexts and perceived motivations behind those exploiting information technology opportunities. Their narrative is thus analyzed and interpreted within the realm they consented for.

4.4. About Research Participants

A total of 22 individuals participated in the study. These research participants spanned various disciplines and backgrounds: seven worked in anti-virus companies in various positions such as threat intelligence or malware reversing, four in banks as cybersecurity specialists, two in threat intelligence companies specifically targeting groups behind online economic crime, two for government agencies looking at online threats targeting public facilities, two as journalists specialized in technology and crime, three as independent contractors (one penetration tester, one forensic specialist and one malware analyst), one as the head of communication for a cybersecurity company and one as a malware researcher who didn’t specify the company nor the sector he worked for.

The geographic diversity of research participants is also diverse: four were Mexicans, three Russians, three Romanians, three French, two Taiwanese, one Ukrainian, one Czech, one Greek, one English, one Indian, one Chinese, and one Argentinian. Since research participants are quoted below and linking their nationality with their position could deanonymize them, I do not provide further information on who is from where.

The large geographic representation of research participants was done on purpose: to uncover factors and perceived motivations that crossed borders and cultures and avoid bending the results for a single geographic region. However, the diversity in experts' professional positions and respective subfields was rather an artefact of the Laboratory's network**.** In the end, the diversities in background, positions, and subfields provides strength to the overall narrative, as themes that span countries and expertise illustrate powerful global trends that can help understand why and how individuals participate on online economic crime worldwide.

4.4.1. Experts' Knowledge on the Topic

What gathered research participants together was their knowledge and stories of individuals involved in online economic crime. A total of 64% of experts had discussed, in the past, with individuals involved in such activity. For example, some of them knew these individuals from social ties, such as going to school with them. Others went undercover, most of the time in forums. Two experts interviewed individuals involved in online economic crime as a function of their job. One expert even ended up hanging out with a group involved in credit card theft. In two cases, experts were contacted by those involved in the crime to explain why they were conducting their crimes, as opposed to experts reaching out to them. A few reported having participated in online criminal activities "back in the day". This should come as no surprise. In the cybersecurity field, there are several accounts of individuals "testing the technology" before finding full-time legal jobs (Tanczer, 2019; Lusthaus, 2018). Those who did not have experiential knowledge (36%) had conducted in-depth investigations of individuals involved in IT-related crime.

All in all, all experts had extensive knowledge on the topic, either through their professional position or their extra-curricular activities. They told real-life stories of individuals involved in online economic crime and shared their impressions on what contextual factors and perceived motivations could influence individuals to participate in such activities. The term "perceived motivation" is used since many accounts are based on experts' interpretations of what motivated those behind the crime.

4.5. Analytic Strategy

The narratives that emerged during the interviews were constructed from the questions asked, the experts' knowledge, and the online interactions. Each interview was transcribed and anonymized. Then, the transcript was imported into the NVivo 12 software for analysis. An **inductive thematic analysis** was conducted to find patterns and meaning in the text. No preliminary codes nor preliminary themes were established. I also did not look at the literature on the topic, something that was done later in the research process. This strategy was taken to let the themes emerge from experts' understanding of the contexts and perceived motivations that influence individuals to participate in online economic crime, rather than from predefined knowledge and theories.

Thematic analysis is a method to identify, analyze and report themes representing meaning from text data (Braun and Clarke, 2006, p.79). Themes can be identified at the semantic or latent level. More precisely, at the semantic level, researchers look for specific patterns in the data, based on what is said, and do not look beyond. The themes are then summarized and the interpretation and relation to the theory is conducted afterwards (Boyatzis, 1998). At the latent level, researchers go beyond the semantic context, reporting underlying ideas and assumptions experienced by the individuals based on their conversations and the researchers' interpretations of such conversations (Boyatzis, 1998).

The themes were extracted at these two levels: semantic and latent. Semantic-level themes included those summarizing perceived motivations and contextual factors behind online economic crime. When I ended up interpreting further how experts perceived the organization behind those involved in online economic crime, the themes were extracted at the latent level.

In terms of process, the text for each interview was broken down into narrative units: groups of words that make sense together. Then these groups of words were associated to subthemes. Once all interviews had been analyzed, subthemes were grouped into overarching themes.

4.5.1. Experts' Quotes

In the results, the themes and subthemes are supported with quotations from experts. For anonymity and confidentiality, each expert quotation is accompanied with the interview's internal ID, such as Expert 0000. The context in which experts expressed their thoughts is, to the best of my knowledge, respected. The language barrier also sometimes led me to paraphrase their statements to facilitate the reading experience. One difficulty was to give everyone fair representation in the results, as some interviews had more content than others. In the end, I used at least one quotation from each participant.

4.5.2. Researcher's Position

As the qualitative approaches are diverse and complex (Holloway and Todres, 2003), the quality of such studies depends on "methodological skills, sensitivity, and integrity of the researcher" (Patton, 2005, p.1). To provide transparency on the research process, this subsection outlines my epistemological and personal positions.

To avoid falling in the "theory-as-ideology" trap (Roulston, 2001) researchers must reflect, acknowledge, and outline the epistemological position of the qualitative research they conduct, depending on the approach used. Such acknowledgment is scarce in quantitative research, while qualitative research cannot escape the active role of a researcher in the data collection, analysis, and result reporting process. The epistemological position of this research is a post-positivist one: science can develop warranted truth claims about the world, despite these claims being fallible (Hicks, 2018). Such fallible claims are not objective knowledge on the strong sense. They rather embody objective knowledge on a weak sense: they are developed through intersubjective agreements. This position recognizes that scientists embody a subjective outlook on their research and only through strong inter-agreements with other scientists, warranted truth claims can be made about the social world studied (Hicks, 2018).

When conducting qualitative research, researchers are also encouraged to take on a reflexive process and acknowledge how their views of the world may influence qualitative results (Watt, 2007). My subjective outlook is formed by three experience milestones: 1) experience in the private sector as a cybersecurity researcher; 2)

graduate studies in criminology; and 3) undergraduate studies in economics. Through these past experiences, I developed a critical approach towards the way crime and information technologies are depicted by the industry, the media and academia. Such depictions are often filled with metaphors (e.g., the cyberspace metaphor), fear narratives (e.g., cyberwarfare) and overgeneralization (e.g., everyone can hack from anywhere). The data analysis and resulting themes found are thus influenced by this critical perspective.

4.6. Ethical Considerations

This research has been approved by the Simon Fraser Ethics Department under minimal risks (study number 2020s0121). Research participants received a consent form prior to the interview. Before the interview, I also inquired whether they had received and read the form and, if not, we went through it together. To preserve participants' anonymity and confidentiality, the participant's signature was not requested. Participants were also told that their participation in the study is voluntary and that they may withdraw from the study should they choose to do so. The collaborators' institution, the Czech Technical University, has also given ethics approval for this research.

Chapter 5.

Experts' Perceptions: Contexts, Motivations and Organizations

This chapter presents the common narratives that emerged from the interviews. The research question driving the interviews was: "*What are the contextual factors and perceived motivations behind online economic crime?*" The chapter starts with a collection of five stories reported by five experts. Then, the results of the thematic analysis are presented. These results are divided into three sections: 1) a confluence of contextual factors, 2) perceived motivations, and 3) perceived structure of groups behind online economic crime. The third section, "perceived structure", is the result of the inductive thematic analysis which led me to depict how experts perceived the organization of those behind online economic crime.

5.1. Five Real-Life Stories of Online Economic Crime

To begin, a collection of five stories reported by five experts is presented. These stories are not ground-breaking cases that made international news. Instead, they are typical stories that illustrate the experiences of different individuals who ended up involved in online economic crime. They are presented first to illustrate what experts had in mind when they expressed their thoughts throughout the interviews.

Exiled Soldiers

An expert talked about a group of ex-soldiers that were exiled from their own country because of a political crisis and ended up with no nationality. Yet, "with their discipline and strong will", they started to participate in underground forums, learning how to steal cryptocurrency wallets and credit cards. The scheme grew big enough so they could buy a few houses and send money back home. To manage more complex operations, they hired individuals with high technical skills from schools. They also recruited young individuals from the street to cash out and launder their stolen money. They ended up forming an organized criminal group conducting various online economic crimes.

Trapped IT professional

A security engineer started working for a small criminal group due to better financial potential. He ended up the technical administrator of a large-scale banking operation, stealing millions of dollars. The pay was 1,200 euros per week, a high salary considering his home country. He changed his way of living, borrowed money from a criminal source, moved with his family to the country where the group operated, and built a house based on that base salary. After a while, the boss of the criminal group behind the operation became aggressive and threatening to him, but by then the security engineer was trapped: he could not make such a salary in the legitimate realm and he was facing recuring payments for the house and the criminal loan he had taken. Depression and household conflict ensued, according to the expert telling this story.

Gaming and Youth

A young individual loved gaming. While playing, he met a girl and started chatting with her. She sent him a link with a pack of emojis which, once clicked on, started interfering with his computer: opening the CD player, exposing his IP address, and locking him off his device. He promised to himself that this would never happen again and started learning computer security. While gaming, someone “DDoSed” (sent a large number of requests to a website server until it shuts down) the game server, preventing anyone from playing. The young individual became angry and started talking with the *DDoSer* to understand the attack technique; the conversation led him to join an Internet Relay Chat (IRC) on hacking. This was a small community of like-minded young individuals who tested the limits of various technologies together. He eventually became the leader of that community, building and managing botnets, stealing credit cards, and developing sophisticated schemes to buy technological products he could not afford at his young age. This lasted for a few years, and he eventually was hired in cybersecurity. He is now a strong advocate for online capture-the-flag competitions.

Subsidies Zoning Fraud

A database manager used to work for an institution keeping track of zoning information for government subsidies. Depending on the zoning level (e.g., zoning A), more subsidies are granted for economic development. Through a personal relationship with another employee, he managed to re-access the institution’s database from that employee’s laptop, pivoted in the company’s network, escalated his privileges, and

established a persistence mechanism, allowing him to access the database whenever he wanted. With this access, he developed a consulting business with a high success rate winning subsidies on geographic profiling for entrepreneurs. After a while, he made so many changes in the database (illustrating that he was highly confident that he would not get caught) that a security system triggered, leading to a forensics investigation and, eventually, his arrest.

From Traditional Robberies to Carding

For many years, a criminal group successfully conducted several robberies. Once the scheme did not work anymore, the group pivoted to online economic crime. Group members participated in credit card skimming (using a device that steals credit card numbers), and banking credential theft through social engineering. They recruited many individuals in the credential theft scheme, training them to call potential victims and impersonate bank representatives. However, group members were not aware of all the traces they left behind while conducting their online illicit activities, due to their lack of technical skills. It still took about two years and many complaints for the whole scheme to be taken down by law enforcement.

5.2. A Confluence of Contextual Factors

These stories depicted various schemes and experiences behind online economic crime. This section presents the contextual factors that emerged through the thematic analysis. For clarity purposes, “factor” refers to *circumstances* that contribute to a result and “contextual” is the *environment* in which individuals evolve. Contextual factors are circumstances, identified at the environment level, that can explain why individuals end up participating in online economic crime. The assumption behind this analysis is that *there exist common contextual factors that can explain why many individuals participate in online economic crime.*

From the thematic analysis, three contextual factors emerged: (1) lack of legal economic opportunities, (2) lack of deterrents, and (3) means of drifting. These factors represent a cocktail that, all together, creates favorable contexts that could influence individuals to exploit online economic crime opportunities. They are presented below.

5.2.1. Lack of Legal Economic Opportunities

Throughout the interviews, the lack of legal economic opportunities was often mentioned in experts' narratives as a contextual factor influencing individuals to participate in online economic crime. For example, Expert 1200 mentioned that in a specific context where such crime is prevalent: "*You can count on your fingers the security companies that we have on the defender side. And the thing is that there are other local companies, which are not paying enough.*" Expert 1300, in the same vein, mentioned that it is *"very hard to be employed in this field I guess"*. More bluntly, Expert 402, when talking about an individual involved in economic crime, said: *"He lived in the country where you don't have much money, even if you are a security engineer, your paycheck is like shit."*

Expert 901 did notice that those living in the countryside were more likely to end up in such activities: *"If you live in a small city, then, even if you're smart enough, you might not be able to have a good job in that city"*. Expert 401 talked about the rate of unemployment in specific districts that may explain why some individuals end up accepting quick online economic crime contracts, such as being a money mule: *"the fact that the rate of unemployment in those districts is very specific, very high. So, it's way easier to recruit mules in those districts"*. Experts 1001 and 100 also mentioned the fall of the Soviet Union that led to high unemployment rates, which, mixed with high technological development, have led individuals to seek online crime opportunities. Expert 200 mentioned inequality, recalling that the individuals he investigated came from unequal societies. He stated that those in poorer conditions (where there were few legal opportunities to make decent salaries) were more likely to seize online economic crime opportunities.

However, experts also stressed that such a factor does not excuse these behaviors and that participating in such activities is more a choice than a necessity. For example, Expert 900 mentioned: *"if you want to have a legal job, there is always a way of you getting in […] Yeah, there is a way of doing some remote work. Actually, nowadays it's easier."* Similarly, Experts 901 and 1200 mentioned the possibility of using bug bounty programs to earn money by legally finding bugs in software. Expert 901 goes as far as staying: *"There is always a way out. People just don't see it. Or don't want to see it."* Individuals do not necessarily participate in online economic crime to survive,

although the lack of legal economic opportunities may be the factor that influences them to choose this opportunity over another legal one.

5.2.2. Lack of Deterrents

The second contextual factor, lack of deterrence, refers to the lack of measures or practices aimed at discouraging individuals from conducting online economic crime for fear of retribution or consequences (be it formal or informal). The lack of deterrents usually expected from law enforcement agencies, justice systems or peer judgements was mentioned by several experts. The absence of these deterrents provides a feeling of impunity to individuals involved in online economic crime.

For example, Expert 1300 stated: *"you can realize that they [individuals involved in online economic crime] do not care, because no one in this country has ever been jailed for doing something bad in cyber*", while Expert 300 mentioned: *"the local institution which investigates economic crime is still really, really badly organized".* Expert 500 also mentioned how law enforcement needed to "level-up their game": *"Yes, I think we need to improve our investigation capability to figure out what, and who, are the bad guys."* Expert 401 revealed how one individual involved in online economic crime texted him: *"Okay you know, law enforcement in [country] they really suck at their job".* That same expert added:

> "When we decided to fight back against this guy, I spent hours and hours and hours with the law enforcement trying to explain how the business works, how the guy works, etc. It was for one guy, only for one guy. Honestly, I spend days with law enforcement. And I will be called again in the future to do that, to explain, in front of a judge, how the business works, all the money laundering works, etc. I accepted to do that but it's a lot of time burned for almost nothing, you know."

Expert 1103 mentioned*: "We know that the police enforcement doesn't have the skills nor the people to catch anyone doing anything"*. This feeling of impunity due to law enforcement inefficiency is mentioned quite bluntly by Expert 700 when talking about the organization behind online economic crime: *"So I think they're quite aware of that. I don't get a sense that, in terms the more organized crime, the cash motivated cybercrime. I don't get the sense they have any fear about law enforcement whatsoever."*

Law enforcement misaligned incentives were also mentioned as an explanation of law enforcement inefficiency. For example, Expert 1001 said: *"One, law enforcement individuals need to know. Second, they need to care. And third, they need to do something, and they probably have other more pressing issues."* Expert 901 discussed how investigators are less likely to open an investigation in their country if there are no victims, allowing individuals to target victims abroad without the threat of law enforcement. This is reiterated by Expert 700:

> "Most of your job as law enforcement is about your local area so whether it's your local region or your country. If there is a hacker in a foreign country who is targeting people in your country […], even if you get that person arrested, it's not going to count towards your arrest figures, because they were arrested by Indian police or by Sri Lankan police for example."

Expert 502 also mentioned that some individuals involved in online economic crime ended up moving from their origin country to other countries where law enforcement would not bother them. These individuals thus exploited loopholes across jurisdictions. Corruption was also raised by experts. For example, Expert 1300 mentioned that there is no deterrence: *"because they know they can like pay money not to be jailed and to get this question solved."* Expert 1001 also stated that, if ever you feel threatened by the police, *"You could also bribe them [law enforcement officials]. That's normal."* As stated by Expert 1100: "*If a policeman arrests you for something, you can give him some money to let you go and he will accept it*".

In terms of peer judgements, Expert 1300 mentioned that the absence of negative peer judgement may also be a factor influencing individuals: *"It's an unsaid rule, not to judge a person at all […] It's just none of your business".* Expert 600 mentioned that individuals committing online crimes considered that their actions were legal based on their own moral values: *"it was legal to us"*.

5.2.3. Drifting Means

To get involved in online economic crime, one must start somewhere. Experts discussed various encounters (both in person and online) wherein individuals discovered that participating in online economic crime is possible. These encounters included, for example, knowing friends of friends, school recruitment, online advertising, and gaming.

The drifting means factor represent the third contextual factor that influence individuals to participate in online economic crime, the factor that leads to crime participation.

Drifting by knowing a "friend of a friend" was a common element mentioned by experts. For example, Expert 402 said: *"You always have a friend of a friend of a friend who's doing something weird, and you can have money, if you need something just ask… Social friend or a friend of a friend."* Expert 300 even referred to Granovetter's (1985) theory of strength of weak ties and stated: *"it's not necessarily your closest friends but someone who knows someone who knows someone..."* who leads one to be involved in such activities. Also, being recruited at school was often mentioned by experts. For example, Expert 402 stated that some individuals *"are just students and they are recruited [by groups involved in online economic crime] every year on different campuses".* In an extreme example, Expert 800 said: *"There is some department at Technical University which is full of hackers groups, great ones, and they recruited some of these guys to help them build these online operations."* On a more personal level, Expert 100 mentioned that someone tried to recruit her engineering friend to write malware at school: *"He was studying with a guy who tried to recruit him to write malware".* Expert 300 also mentioned that, at her high school, individuals were actively recruiting students to participate in illicit online activities, as the school was well-known as a good computer science school at the national level. Alternatively, Expert 800 mentioned that criminal groups involved in online economic crime recruited individuals straight from the street. He gave an example of a person he knew who:

> "[…] was just jogging in the street and they [individuals from the organized group] noticed that his clothes were kind of old, so they understood that he can be one of the guys. And they turned him into the money mule, actually."

Drifting through online means was also mentioned. In fact, many statements referred to online recruitment through online advertising using legitimate, well-known channels and platforms. Expert 402 supported this idea quite clearly*: "They look for people who are looking for jobs in famous job websites".* Expert 401 also mentioned*: "They are recreating news on Instagram, mostly. Saying, okay you want to make some money okay create an account in that bank".* Even the large French job website Poll Emploi was leveraged, according to that same expert: "*They successfully created an account on the Poll Emploi website and posted the job offer and I guess they successfully recruited mules from the National Job Offer web portal".*

Expert 402 talked about how online advertising is used to recruit freelancers and employees with ads like: *"You want to work for a remote company with commission? You will receive the money and you will have to send the money back somewhere and you will have a commission with the money transferred"*. Expert 900 stated bluntly: *"There are a lot of online jobs and they're posted by cyber criminals,"* as well as *"I mean, if you see the online jobs, it's easy to see some things that are fishy because usually they pay more than others and they don't have proper contacts",* meaning that they will ask to be contacted via informal networks like jabber, ICQ or Proton mail. Expert 901 also said: *"Actually we saw a lot of postings on job sites searching for a good developer with knowledge of low-level Windows architecture, and yeah, it looked shady."* Expert 1101 similarly mentioned seeing postings online for job offers to recruit individuals in criminal activities. Expert 401 told a story where a woman told him:

> "Okay, I got a job offer, you know, and someone is asking me to translate that message, but I am not sure it is legal and can you give me some advice. And it was a message about that ransomware targeting *la Gendarmerie Nationale*, you know!?"

The woman was thus interested in a translation job offer that asked her to translate a ransomware note targeting the French police! On the other hand, Expert 1102 talked about constantly receiving social network messages asking him if he would be willing to do some "extra work", which was clearly illegal according to him, such as: "*Hey, I like your skills, I like your history. I know who you are. And I would like to propose you with a deal*". This expert illustrated that online recruitment may not be only passive, via online ads, but also active, with individuals messaging others with interesting shady offers.

Finally, online gaming also seemed to represent a means of drifting towards online economic crime. Expert 700 mentioned: *Look, I know computer gamer sounds weird and sounds niche, but you've got to realize this is the training ground".* That expert discussed how there is a crossover between gaming, hacking and online economic crime. Gamers want to hack the game they play, and their curiosity leads them to underground forums and down-the-rabbit-hole of participating in the community and conducting illicit rent-seeking activities. Expert 402 corroborated this hypothesis, mentioning*: "So in Germany, so it's mostly kids and as you said they played Minecraft and they have to DDoS the server to each other and quickly you understand that buying a stolen credit card is super easy".* Similarly, Expert 900 mentioned:

> "All right, like a lot of young people, they develop malware for games. And then they never get caught. And then a few years pass, and they start to do malware stuff, stealing credit cards and things like that."

Based on expert narratives, these three factors, lack of legal economic opportunities, lack of deterrence and having a means of drifting explained why some individuals may end up in online economic crime. These three factors are not necessarily mutually exclusive nor required, but the three all together may increase the proportion of individuals involved in these activities for most contexts. The following sections looks at perceived motivations.

5.3. Perceived Motivations

Throughout the data analysis, experts also mentioned potential motivations driving those behind online economic crime. These included financial gains, and, to a certain degree, the feelings associated with committing such crime, such as pride, excitement, or power. Both perceived motivations are presented below.

5.3.1. Financial Gains

According to experts, there are no doubts that actors behind such crime are motivated by money. For example, Expert 100 mentioned: *"It's all about money, of course",* while Expert 1000 said: "*Why do people go into this illegal stuff? Why do they try to do it? 90% of the time it's about money*". Similarly, Expert 1103 stated: *"Most of them, their motivation is financial. They want to profit from this,*" and Expert 1200 said: "*The main factor is the money*". Expert 1102 mentioned: "*For money, because you need to make some easy money*" while Expert 1100 stated: "*The money I think is the motive*". **It is this finding that led me to consider experts' narratives through the lenses of online economic crime rather than "of exploiting information technologies opportunities".**

What may be more interesting is: how much money? Expert 500 said: "*Yes, I think they are rich*" and Expert 900 mentioned: "*They're very rich*". Person 1101 talked about a group behind ATM skimmers that made millions and reinvested the money in the legal realm, emphasizing: "*I mean, we're talking about a lot of money.*" However, an alternative narrative also emerged across experts' discourses, one that considered those

behind online economic crime as not necessarily extremely wealthy, but rather wealthy enough. These experts stressed that, objectively, the amounts were not, in their view, enormous, but, from the perspective of the individual doing the crime, the amount looked substantial enough. For example, Expert 1200 mentioned: "*I would not say rich. I would say successful enough,*" while Expert 401 stated: "*They make shit tons of money […] but they are not rolling in Porsches nor flying in first class. They can brag with an iPhone, because an iPhone is 1000 euros not 50,000 euros, you know*". That same Expert also added: "*They still make more than normal people but it's still very little. Let's say, you cannot buy a big house, but still a nice one*". Similarly, Expert 100 mentioned that, given specific contexts, the money earned through online economic crime is not necessarily that impressive, but usually more than what individuals would make as a cybersecurity expert in a legitimate industry. Similarly, Expert 1102 stated that, for a specific task related to online economic crime, an individual can be offered more than what he or she would expect in the legal realm: "*like 1200 dollars. Yeah. I mean, it is really cheap. It is really for the American side. For [country], it's another salary range*".

Expert 1300 had a more pessimistic narrative because, according to him, many people involved in such activities were rather poorly paid: "*People who develop malicious code are very often being underpaid*", and adding: *"So, it happens that coders are underpaid. Yeah. I do know like at least two examples of those. But how much? It depends, I guess, it's like a market level.*" When talking about the proportion of individuals making large amounts of money, Expert 901 replied: "*Super small. […] Because then think about it as you would see like everybody with yachts and stuff."*

Thus, the motivation is money, but whether such activity pays depends on one's perspective and context. Potentially, the *idea* that online economic crime yields substantial amounts of money is what drives such criminals, as Expert 900 mentioned: "*they want to be rich cybercriminals*".

5.3.2. Feelings

Money is the perceived overarching motivation for such crime. Yet experts also mentioned motivations that were beyond financial purposes. The motivations that emerged from the narratives were often related to *feelings* or *emotions* experienced when conducting such crime. For example, an individual involved in economic crime

told Expert 402 that: "*At first, it's not about the money, it's about the adrenaline that I can have when I'm able to like steal money from somebody*". The most common feelings mentioned by experts included pride and fame (attention seeking), excitement (such as adrenaline kicks) and having power over others. These emotions were related to the act of defrauding individuals for economic purposes, such as individuals hacking into companies to launch a ransomware. Each of these emotions are briefly presented below.

Experts mentioned that taking **pride** in the illicit activity can be considered a motivation. For example, Expert 401, when talking about an individual developing a banking trojan, stated: "*He was very proud of himself. He really wanted to show the people to show everyone, Okay, I did that, I'm pretty good at what I'm doing, and you know you guys suck and I'm the best etc.*". Similarly, Expert 700 also stressed such feeling, mentioning: "*It's a creation, and it takes skills, and it takes patience, and it's something that they're struggling, I think, with the pride that they feel in what they created*". Such a feeling was also expressed by Expert 200: "*The biggest motivator is money, and after this is the feeling of doing something like create a name in the underground scene.*" Pride involves peer recognition, and subsequently **fame**. Expert 1102 stressed that fame, a close relative to pride, is a motivator: *"It is fame*" and "*they actually work to be famous*" while Expert 700 similarly mentioned: *"You can see people that are saying [in forums] I'm the guy who did this or you know, I recognize you from such and such. There's a need for fame in there."* Similarly, Expert 800 talked about a group he interacted with that *"were really proud. Yeah, they are considered the heroes in their villages they were born, because they made it to the big world, and they are making a lot of money*".

Apart from seeking pride and fame, the **feeling of excitement** was also expressed by experts, excitement for specific actions such as writing malware and infecting devices for economic crime purposes. Excitement encompasses pleasure, fun, joy and adrenaline rushes. For example, Expert 402 mentioned that an individual developing banking trojans he interacted with kept experiencing adrenaline rushes. Expert 600 also mentioned how doing such things may be motivated by "*the drive, or like the kick, you get in doing such things,"* while Expert 700 said: "*It's just, you are throwing yourself again and again and again at a closed door for the joy of the one moment when the door swings open.*" Experts perceived these emotions -which was gathered into the

excitement subtheme- as motivators behind online economic crime. Finally, within experts' discourses, **having power over others** seemed to be a dominant motivator that influenced individuals behind such crime. For example, Expert 800 mentioned:

> "I think the feeling or idea of being important or to have power over some other people. And this fascinates them because all they can do is just sit behind the computer. And while doing this, they have actual power controlling other people's systems."

while Expert 600 said: *"It's the capacity that you have to keep learning over others and having knowledge is addictive. When you can show that you have knowledge."* Similarly, Expert 300 mentioned*: "I think they just enjoyed the power and the control, and I guess it in an increasingly connected world, being able to play with this kind of stuff is sort of a high power".* The idea of having power or control over others while participating in online economic crime was a recurrent theme in the data.

5.4. The Perceived Structure of Groups behind Online Economic Crime

The semi-directed nature of the interviews and the data analysis following an inductive approach yielded unexpected results as I ended up sorting different perceptions on the organization of online economic crime. Throughout the interviews, how experts perceived or conceptualized the organization of online economic crime varied greatly, both across experts and within an expert's discourse. Four organization types emerged from their discourse. Two that referred to somewhat structured organizations: (1) criminal groups with a certain degree of organization and (2) enterprises. Two others that referred to more organic associations: (3) networks and (4) communities. Each of these organizations is presented and discussed below, providing an interesting depiction of how criminal associations behind online economic crime are understood by experts.

Moreover, this perspective sheds light on the importance of "indispensable workers" within experts' discourses: individuals who are key to the organization of online economic crime regardless of the perceived structure behind these groups. Such indispensable workers conduct all daily mundane activities surrounding these kinds of crimes, such as calling victims to social engineer them, managing infected servers, or transferring money (i.e., money mules). Mentions of these workers are presented below.

5.4.1. Structured Organization

The structured organization mentioned by experts includes **criminal groups with a certain degree of organization** and enterprises. The first type refers to groups of individuals who know each other from the “offline world”. These groups have well-defined roles related to their involvement in criminal activities. From this type, t**wo subtypes** emerged: groups that formed due to early online crime opportunities and more “traditional” criminal groups who now seek such opportunities.

The first subtype, **groups that formed due to early online crime opportunities**, refers to groups that started a while ago: at the birth of the democratization of information technologies. Consequently, they are nowadays knowledgeable on online money-stealing processes and techniques. Expert 901 depicted them as *“more mature criminals, actually criminals who know the drill and who know how to organize this pyramid of people and how to actually make money out of it,”* while Expert 402 stressed their maturity: *“From everyone I saw, it’s people aged forty+. Nobody under forty I saw”*. Similarly, Expert 200 argued that such organizations are formed of *“Old kind of people; you know that they have not just graduated from University but are rather part of an organization that has been known for a while”*. The relative size of such groups, in terms of the number of people, is also perceived as limited. For example, Expert 900 mentioned that*: “when one of them [crime groups] gets caught, you can count them on one hand”*. Similarly, Expert 402 mentioned that, considering only Russia, the sum of individuals involved in such groups represents fewer than 100 people: *“like those people who will take the lead and are the top of the top, those people are the very few”.* However, these individuals seem to be very successful at what they do, explaining why they stay within such a business for many years, according to experts. For example, Expert 900 mentioned*: “They're very rich, they have the resources to do this [sophisticated criminal schemes]”.* Similarly, Expert 402 said that these groups are the ones we hear the most about; they are the ones “*making one or two million a month”* and they meet “*in yachts and big hotels and pictures of their parties with cocaine and drugs get leaked to the media”.*

The second subtype refers to **traditional crime organizations seeking online crime opportunities**. The story, presented above, of a group specialized in robberies that then pivoted to credit card skimming (using a device that steals credit card numbers)

once robberies were no longer successful is a good example. In the same vein, Expert 901 mentioned that, in many cases, when a criminal group was uncovered*, "Several members came from traditional crime".* Alternatively*,* Expert 1103 talked about how traditional drug cartels are now recruiting tech savvy individuals, stating: "*So basically a lot of drug cartels here in [country] are so interested [in technical abilities], they find that they need to recruit these kinds of guys*".

The second type of structured organization perceived by experts was as **enterprises**. **Two subtypes** emerged as well: groups organized as enterprises or actual enterprises involved in online economic crime. The first one **referred to criminal organizations with paid employees and a structure similar to that of an enterprise**. For example, Expert 402 talked about an individual working as an employee for the criminal organization *"to steal from banks from different countries and have a commission, a salary".* Similarly, Expert 901, when talking about an individual developing malware for a criminal group, mentioned that the work was like a *"day-to-day job"*. That same expert referred to individuals responsible to cash out money as *"low-level personnel"*, using the word "*personnel"* and so reflecting the idea of their being enterprise workers. The story above of the "trapped IT professional" also reflects this perceived structure. Expert 1001 went even further in the analogy, mentioning that those behind online economic crime *"are organized just like normal companies with CEO, CTO and marketing departments."*

The second subtype comprised **actual enterprises involved in online economic crime**. Expert 400 experienced an attack on infrastructure and, once investigating the threat, found that the organization behind it was a legal company. The criminal scheme involved sending lots of spam that:

> "pretended that you had a parcel to be delivered to your house, written in [language] and faking the company's logo [the company the expert worked at]. The spam required that the individual dialed a special number that charged 2 euros to get a code. The excess charges were sent to a legal company, which, according to a press release describing the arrest of the company's boss and seven employees, summed to 1.5 million euros per month."

An analogy of companies with a double identity, legitimate activities and illegitimate activities was also found in the discourse of experts. For example, Expert 1001 mentioned *"[…] there are companies in Russia that have, for instance, two floors.*

One floor is a legitimate tech business, and the other floor is a non-legitimate tech business". Expert 1200 also talked about double-identity companies subcontracting individuals who *"are not aware of the company's operation or whatever the company is doing."* because *"they are not actually aware of this stuff, whether it's legal or illegal since they are like a kind of employee for that company. For them like they are just getting money to do that job."* Expert 1100 similarly told a story of a legal enterprise that installed ATMs across a city with skimmers (credit card theft devices) built into them. By the time the enterprise was caught, the money had been stolen and reinvested in the legal sphere.

5.4.2. Organic Structures

Organic structures included two types: **loose networks of entrepreneurs** and communities. For the former, experts sometimes perceived the organization behind online economic crime as loose networks of entrepreneurs seeking to associate for business opportunities. Such discourse was tied to the idea of specialization (referring to separation of tasks in the market) and how online platforms may be used to find business associates. For example, when Expert 901 discussed the organization behind online economic crimes, he mentioned the separation of tasks; for instance, *"the programmers are completely disconnected from the people who are selling it actually"*. Expert 402 expanded on an individual who developed a banking trojan that targeted French banks. That individual started by selling *"his malware, but he was mocked on different forums. So, he decided to run his business with his own […] and started making a lot of money".* According to the expert, that individual moved to Ukraine and found a way to buy fake identities and passports, as well as ways to launder the stolen money through mule accounts. He was an independent entrepreneur with a good network.

Experts' narratives also encompassed organizations formed of online **communities**. There were several mentions of "*attacker community*", "*underground hacker community*" and "*there is a big community, you know, people who write malware and they are teaching for free*" (Expert 900). Some of these underground communities are exclusive, as Expert 901 mentioned: *"The real business is happening in the underground forums, which is hard to access"*. Similarly, Expert 401 stressed that "*You have to prove yourself to enter this kind of stuff so it's very difficult for any company or for any guy like me to enter in those*". These exclusive communities are imagined as a

place where entrepreneurs can do "*serious business*" rather than "*sell already hacked computers, already stolen cards and stuff like that.*" (Expert 901). Expert 901, in the previous statement, refers to underground platforms that are open. Other communities mentioned by experts were less profit-driven and more knowledge sharing, like the statement above referring to individuals teaching each other for free. Expert 600 also talked about a community where *"a lot of methodologies on how to get money was shared"*, and the person in that community said: "*This was the first time that I felt in a community. […] I do not know. It was really nice*".

Overall, these four types (criminal groups, enterprises, loose networks of entrepreneurs, and communities) summarize how the organization of online economic crime was depicted by experts. Most likely, the ground-truth lies in a mixture or a blend of these organizations, as discussed in Chapter 12.

5.5. The Indispensable Workers

Additionally, from experts' narratives, I noticed that the various structures perceived seemed to be dependent on a population of individuals evolving at the periphery, the indispensable workers. These workers are individuals who accept jobs from these organizations and end-up contributing to online economic crime. They are not the motivated offenders behind the crime, those who have thought of the whole scheme, but rather a necessary instrument or a needed accessory for the scheme. The concept encompasses a wide range of individuals, from information technology professionals seeking work contracts to translators (like the woman who responded to a job offer on Poll Emploi) to those transferring the money (i.e., money mules). Indeed, several experts mentioned how one could end up involved into online economic crime by accepting contracts that could be considered legitimate at first. For example, Expert 901 mentioned that groups behind online economic crime "*hire, like pentesters and those people [penetration testers] they do not know that they are actually doing cybercrimes".* Similarly, Expert 300 mentioned:

> "Yeah, perhaps you just do a little job for them first and you get paid, and you don't really know that you've done something illegal and then it's like, hey, it's just a gray zone, or they won't really deny that money, and so on. And, yeah, it's a step by step, kind of thing."

Slowly, these individuals may drift into crime, as mentioned by Expert 1300:

> "Some of them have started their activity unconsciously, as a freelancer. So, they were just sort of, you know, advertising their services and someone has contacted them. And they started to work and after that, they realized what was it like, and... But there was no sense to sort of give it up."

Such depiction was corroborated by Expert 900 who stated: *"They give you, like some testing tasks. You do things, they pay you. And they, and then they say, okay, we are doing something different. Like we're doing malware*". Based on experts' discourses, those actively involved in online economic crime employ workers without being entirely honest on the illicitness of the activities. This is not necessarily surprising considering that certain activities surrounding online economic crime are legal, such as building websites or setting up servers. They are indispensable workers because they are needed to ensure the good running of complex schemes surrounding online economic crime. As Expert 100 mentioned: *"to run a botnet, you need to have servers and all the servers they need to be taken care of by administrators. They need programmers and programmers need to write good code".*

Alternatively, middlemen to hide criminal tracks are also needed. For example, Expert 402 talked about a scheme that bought goods with stolen online accounts and someone was hired as a quality manager to receive the goods:

> "So, you are hired to be a quality manager and you receive packages. You have to open the packages and make sure that everything is right, and you send the packages somewhere else and that is your job."

Money mules also act as middlemen and are necessary for the online economic crime to succeed, as stated by Expert 1100. These individuals are the ones who *"get caught because they leave most traces, and it's easy to find them,"* as mentioned by Expert 901. Expert 700 mitigated that statement, stating that the risks may not be very high: "*Finding mules is not really difficult. Mules will take all the risk, but the risks are not so burdensome".* Similarly, Expert 401 mentioned that, in his experience, mules are not found guilty when caught because of the suspicion that the individuals may not be aware that the money cashed out was stolen.

These workers, be they money mules or IT contractors, illustrate that, for online economic crime schemes to succeed, there may be more individuals involved than only motivated offenders. The implications of these findings are discussed in Chapter 12.

Overall, interviews with experts uncovered contextual factors and perceived motivations of those behind online economic crime, related to the first objective of this study. The inductive thematic analysis also led to exploring how experts perceived the organization of those involved in such crime and the indispensable workers surrounding them. To complement these findings, another perspective is taken: analyzing discussions of individuals involved in online economic crime. **This second analysis will contribute to fulfilling the first objective of this study from a different angle.**

Chapter 6. **Methods for Private Chat Log Analysis**

The following analysis moves beyond experts' perspectives and focuses on a group involved in online economic crime. This was made possible thanks to the Stratosphere Laboratory that gave me access to a private chat log containing conversations among Russian-speaking individuals involved in spreading malicious banking applications related to the Geost botnet.

In short, the **Geost botnet** is an Android banking Trojan botnet that infected nearly 800,000 Russian phones and had access to millions of Euros. It was discovered in 2018 during analysis of the network traffic of the HtBot proxy-malware, a proxy service known to be used for anonymity purposes by individuals involved in crime. The researchers found unencrypted network traffic directed to the botnet's Command and Control (C&C) web server when monitoring the proxy, allowing identification of the botnet's domains and IP addresses as well as its infrastructure and general purpose. The complex technical analysis of the botnet had already been published by members of the Laboratory (see Garcia et al., 2019). It is during this investigation that the chat log containing private conversations among individuals involved in spreading the botnet was uncovered, as explained below.

This unique dataset was used to fulfill the first objective of this study: to uncover the contextual factors and perceived motivations of individuals involved in online economic crime. The research question leading the analysis was: "*What are the motivations and challenges behind those involved in online economic crime?*" The research question focuses on identifying the *challenges*, as opposed to the contextual factors. This allowed me to stay as close as possible to the conversations while understanding the context in which these individuals evolve. This chapter focuses on the methods and data. It starts by presenting the dataset and the study population. Then, the data analysis is outlined along with ethical considerations.

6.1. Dataset

The chat log was found on the Virus Total platform by Veronica Valeros from the Stratosphere Laboratory. Virus Total is a "free service that analyzes files and URLs for viruses, worms, trojans and other kinds of malicious content" (Virus Total, 2020). Anyone

can submit a file to Virus Total for inspection through a public web interface. The files submitted are available to anyone who has an account with them. Virus Total's *Terms of Service* mention that a file submitted on their service should be considered public. For these reasons, the chat log is treated as a public file, although it is accessible to only those who have a paid account with the company. The chat log is an Excel spreadsheet, and the conversations are written in Russian. Over 90% of the conversations were translated by Anna Shirokova, a Russian-speaking researcher who participated in the Garcia et al. (2019) investigation. The remaining 10% was translated using the Google Translate application online.

The chat log was linked to the Geost botnet due to the exchange of specific information that could be known only by individuals actively involved in the malicious operation. Within the conversation, passwords, IP addresses, and specific domains related to the internal operations of the Command and Control (C&C) web servers were shared. Specific information about the Geost Android application packages (APKs) was also distributed, along with how to obfuscate those APKs before uploading them to webpages. The obfuscation method used to avoid antivirus detection of the Geost botnet was completely uncovered and published (Sembera et al., 2021).

In terms of the format, the chat log is formed of 32 conversations and 6,249 messages **between one individual and his business partners**. All conversations were related to business: there were no intimate/personal conversations. Each conversation contained a flow of messages between the main entrepreneur and another business partner. For each message, the specific time and date was available along with the sender's and the recipient's usernames as well as the content of the message in Russian and its translated version (if available). The first message was sent June 11th, 2017, and the last one was sent April 17th, 2018; the dataset thus spans 310 days. Figure 3 shows the number of messages exchanged through time in the chat log. Most conversations took place at the end of 2017 and early 2018.

In terms of frequency of discussions, of the 32 one-to-one conversations, 12 had one message and 9 had fewer than 20 messages exchanged; 5 included between 20 and 100 messages; 4 between 100 and 400 messages; and 2 more than 1,000 messages, forming the core of the dataset. The analysis below centers on the **11**

conversations that had more than 20 messages, encompassing 6,134 of the 6,249 messages.

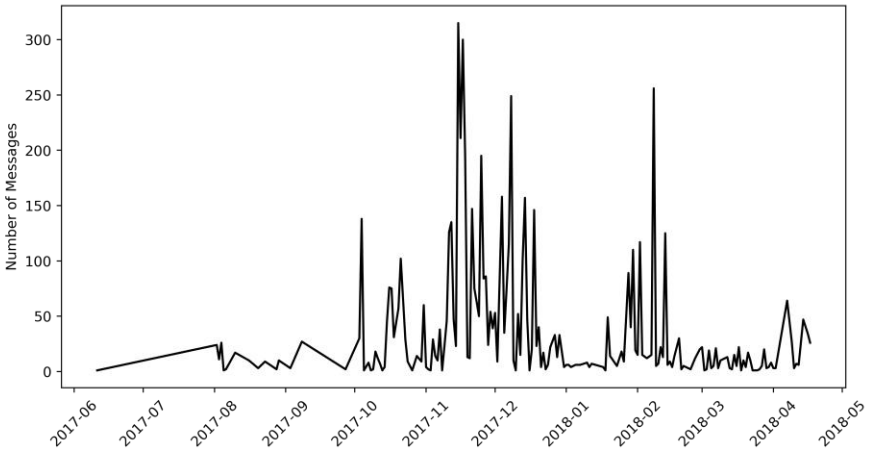

Figure 3 Private Chat Log Frequency of Messages Sent

6.2. Study Population

The **main individual** in the chat log, the one who converses with everyone, is called the “Main Entrepreneur” throughout the thesis. Baumol (1996) defines *entrepreneurs* as individuals who are ingenious and creative and find ways to create wealth, power, and prestige. When focused on innovation and productive activities, entrepreneurs benefit societies by creating wealth. However, entrepreneurship can also be destructive, especially when the entrepreneurs focus on rent-seeking at all costs and engage in tax evasion or unproductive activities to do so (Baumol, 1996).

The main individual in the chat log is considered an *entrepreneur*, as defined by Baumol (1996), because of the economic activities he engages in: creating websites for rent-seeking purposes. He hires and deals with various contractors to increase the efficiency and reach of his websites and participates in various pay-per-install or pay-per-click programs to make money out of them. These economic activities led him, with others in the chat log, to contribute to spreading the Geost botnet.

The other individuals in the private chat log are considered his business partners. Given their conversations, I created **seven roles** that summarize their function in relation with the Main Entrepreneur. They are presented in Table 1.

Table 1 Business Partners Roles Created from the Private Chat Log

Name	Role
Website Master	Individual involved in developing websites as well as taking various strategies to promote them for monetization
Web Developer	Individual paid to develop websites
Affiliate Marketer	Individual involved in managing affiliate marketing programs (such as developing deals with telecommunication companies or running the platform)
Text Writer	Individual paid to write text for better website visibility
Server Cleaner	Individual paid to clean servers when infected with malware
Money Exchange professional	Individual that specializes in money exchanges
SEO Professional	Individual paid to improve website performance for better website visibility

These seven roles were distributed among the **11 business partners**. Each business partner was given one role that summarized best their activities, according to the conversations. In short, two business partners in the private chat log were **website masters** (Website Master 1 and Website Master 2). They were creating websites for rent-seeking purposes, just like the Main Entrepreneur. They discussed various aspects of the business with the Main Entrepreneur. Website Master 1 was also working in close collaboration with the Main Entrepreneur, as explained below.

Two other business partners were **developers** (Developer 1 and Developer 2): individuals hired to develop websites on behalf of the Main Entrepreneur. Two additional business partners were identified as **affiliate marketers** (Affiliate Marketer 1 and Affiliate Marketer 2). Affiliate marketing programs are programs that website master can subscribe to to try to make money out of their websites, such as pay-per-install. Either these affiliate marketers tried to recruit the main entrepreneur to participate in the program or the main entrepreneur sought them out for business opportunities.

One business partner was tagged as a **text writer**. He was hired to write texts on the Main Entrepreneur's websites. Texts relevant to the website's topic can lead to higher visibility on search engines like Google or Yandex. Two **server cleaners** were also identified in the private chat log (Server Cleaner 1 and Server Cleaner 2). They were hired to fix the Main Entrepreneur's server that was hacked at one point in the conversations.

There was one **money exchange professional**. He was contacted by the Main Entrepreneur to exchange money from one currency to another. Lastly**,** there was one **search engine optimization (SEO) professional** who was paid to improve the Main Entrepreneur's website visibility through various SEO tactics, such as click redirections.

The aliases (representing their roles) are presented in Table 2, with the number of messages exchanged between each of them and the Main Entrepreneur, the first date and last date of interaction, and the length of the conversation.

Table 2 Business Partners related to the Main Entrepreneur

In chatlog	N. Messages	Date start	Date end	Conversation Length
Website Master 1	2,043	2017-10-04	2018-04-17	195 days
Website Master 2	74	2017-09-27	2018-04-14	199 days
Developer 1	2,871	2017-10-03	2018-04-02	181 days
Developer 2	33	2017-10-15	2017-10-24	9 days
Affiliate Marketer 1	156	2017-08-23	2018-03-04	193 days
Affiliate Marketer 2	207	2017-08-02	2018-04-16	257 days
Text Writer	30	2017-08-04	2018-01-18	167 days
Server Cleaner 1	355	2017-11-21	2017-12-07	16 days
Server Cleaner 2	22	2017-11-12	2017-11-13	1 day
Money Exchanger	310	2017-09-08	2018-01-19	133 days
SEO Professional	33	2017-12-14	2017-12-28	14 days

As shown in Table 2, Website Master 1 (conducting business similar to that of the Main Entrepreneur) and Developer 1 (hired to develop the Main Entrepreneur's websites) are the two individuals with the highest number of messages exchanged with the Main Entrepreneur. Moreover, information about the Geost botnet was shared within these two conversations. **The Main Entrepreneur, Website Master 1, and Developer 1 are thus, with a high degree of certainty, three individuals who are involved in online economic crime.** The other individuals are subcontractors doing short-term contracts for the Main Entrepreneur. Whether they know the websites are related to illicit activities, namely, spreading malicious applications, is not obvious through the conversation.

The conversations between the Main Entrepreneur and the two individuals involved in such activity formed 79% of the chat log; they are thus the focus of this

analysis. However, interactions with the other nine individuals (and the 21 short conversations) are also analyzed, allowing the gathering of as much information as possible.

6.3. Data Analysis

The conversations in the private chat log were analyzed using a thematic analysis and an inductive approach: no theme was predetermined prior to starting the analysis. The NVivo qualitative data analysis computer software[15] was used through the process. For each conversation, an intervention was broken down into narrative units representing themes, dubbed “nodes” in the computer software. Themes were created and modified as the conversations were analyzed. They were extracted at the latent level (Boyatzis, 1998), as I interpreted the motivations and challenges of these individuals throughout their conversations.

Due to the complexity in the terms used and the difficulty in understanding some of the translated content, each conversation was analyzed and read at least three times. Each time, new meaning was extracted as the flow was better understood. After analysis of each conversation, a summary of the conversation was recorded in the memo area of the software to facilitate remembering the whole flow of the conversation. Once all interactions were coded, a transversal analysis of the subthemes that emerged in each conversation was conducted. The sub-themes were merged into three large themes that best encompassed all sub-themes and topics uncovered. Throughout the results, each theme found is supported with paraphrases from the conversations.

Lastly, throughout the analysis, I faced difficulties in understanding the realities of the individuals studied due to the cultural distance between their reality as Russian-speaking individuals and my reality as a Canadian researcher. Sometimes, the translation was not accurate or was hard to comprehend, and contextual meaning was missing or difficult to assess. Hundreds of hours were spent reading the conversations and trying to find patterns and meaning to them. Although I cannot carve out my subjective outlook on the dataset, I can and do try to report the motivations, and challenges of these individuals to the best of my knowledge. This is done by following

[15] https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home

the methodology mentioned above and re-validating the results by constantly digging back into the data and going over each conversation several times.

6.4. Ethical Considerations

This research has been approved by the Simon Fraser University ethics department under minimal risks (study number 2020s0121), which required asking for a *waiver of consent* in line with Article 5.5A of the TCPS2. To ensure participants' confidentiality and privacy, the pseudonyms of the research participants found in the chat log were not used. Their statements were also paraphrased (rather than giving the exact quotation) to ensure that a quotation could not be easily linked to an individual in the chat log through automatic text search.

Chapter 7.

Private Chats: Dancing on the Crime Line

This chapter start by presenting the themes that emerged through the inductive thematic analysis of the private chat log. The research question driving the analysis was: "*What are the motivations and challenges behind those involved in online economic crime?*" Four overarching themes were found: 1) a hostile business context, 2) amateur work, 3) leniency towards criminality, and 4) seeking economic independence. These themes are presented below and depict the motivations and challenges of the individuals studied. Then, I explain how these individuals are among the **indispensable workers** mentioned by experts. The chapter concludes by presenting the **digital labor platform**, found in the private chat log, that is investigated in the following quantitative chapters.

Before presenting the results, some readers may wonder: *how is the main business of the entrepreneur, which is building websites, related to the malicious Geost applications?* In short, during the period of study, the Main Entrepreneur developed **websites advertised as repositories for Android applications (i.e., Android portals)**. He tried to make money out of these websites by participating in various affiliate marketing programs: programs in which companies pay *others* to advertise their products or services on their behalf. The main programs the Main Entrepreneur participated in were those that paid for downloads of Android applications. Depending on the program's conditions, he could be paid, for example, for an application being installed on a phone through his website or once installed, for every user click on advertising banners inside the application. To attract users to his Android portals and download the advertised applications, the Main Entrepreneur took various strategies, from dealing with search engine optimization firms to hiring individuals to produce content or paying third parties to display links that point back to the websites (known as "buying links").

During the period of study and based on the private conversations, the applications available on the Main Entrepreneur's websites (and the websites owned by Website Master 1) were Geost applications. This means that the applications available on the websites looked benign, like a gaming application, while they were, in fact,

banking Trojan applications[16]. The Main Entrepreneur was paid for each banking Trojan successfully installed through his website by an unknown group of people called “they” throughout the conversation.

7.1. Facing an Adverse Business Environment

The first theme that emerged from the analysis is facing an adverse business environment: the economic conditions surrounding the business are inauspicious. It includes two subthemes: 1) ephemeral and unreliable business partners, and 2) declining business prospects and unstable payments. Each of them is presented below.

7.1.1. Ephemeral and Unreliable Business Partners

Of the 32 conversations in the dataset studied, 27 consisted of short-term conversations with the Main Entrepreneur trying to engage with individuals, without success. Of the longer conversations, the business partners whom the Main Entrepreneur dealt with were often unreliable, a pattern that seemed to be shared within the business context. For example, the Main Entrepreneur once mentioned: “*I can’t launch new sites, programmer disappeared*” (Main Entrepreneur, October 2017) to Website Master 1, who replied: “*I need to write to mine, he did not get in touch for a week*” (Website Master 1, October 2017) and “*Same story, and the programmer keeps disappearing all the time*” (Website Master 1, October 2017). From these interventions, a long conversation ensued about how unreliable programmers are in the business, with the Main Entrepreneur mentioning: “*Well probably he was writing code in his head”* (Main Entrepreneur, October 2017) when referring to files that had been unchanged for a couple of days on the websites’ server.

As another example, the Main Entrepreneur referred a trusted contact to Affiliate Marketer 2, who then mentioned that the referred contact *“[…] just wrote to me and then disappeared”* (Affiliate Marketer 2, November 2017). Similarly, a website developer sub-contracted by the Main Entrepreneur often stopped working for no apparent reason,

[16] This was confirmed through the obfuscation service used by the Main Entrepreneur and analyzed in Sembera et al. (accepted). The service disguised the application as legitimate. However, once installed, the application’s icon would disappear, and the malicious code would run in the background of the victim’s phone.

mentioning, for example: "*If I could understand what is going on, I would have told you. But now I'm saying I am working, but in fact I don't. I am getting demotivated and do not want to do anything*" (Developer 1, October 2017) or "*Hi! I again stopped working on our business*" (Developer 1, October 2017). Following such interventions, the developer sporadically worked until early January 2018, following the holidays, when he mentioned in the conversation: "*Yes, I decided to work, I made one edit, went to the second one, went to the [name] website, sat on the thought, analyzed it. And I think that I will probably refuse the rest of the work.*" (Developer 1, January 2018).

Due to the recurrent problems with the developer, the Main Entrepreneur hired someone else who promised to complete the work quickly. Yet, when the Main Entrepreneur asked for an update, the person answered: *"I have a lot of work on the current active orders, urgent corrections, I don't have time*" (Developer 2, October 2017). The Main Entrepreneur replied that he would wait, yet the conversation stopped. This situation was mentioned by the Main Entrepreneur in another conversation: *"[…] I found one (programmer). He did something for 2 days and then disappeared*" (Main Entrepreneur, October 2017). These examples are not unique but rather scattered throughout the discussions. They illustrate how ephemeral the business relationships are, with individuals frequently changing their minds about the idea of working together.

7.1.2. Declining Business Prospects and Unstable Payments

The conversation illustrated that the business was somewhat saturated, not as good as "*Back in the day*" (Main Entrepreneur, April 2018). For example, when looking for business opportunities, the Main Entrepreneur mentioned he wished he could monetize "*SMS as in good old times*" (Main Entrepreneur, April 2018,) to which Website Master 1 replied: "*There is nothing like this now (smiley)*" (Website Master 1, April 2018). When talking to another business partner, the Main Entrepreneur also mentioned: "*Conversion rate is not very good*" (Main Entrepreneur, November 2017) and "*Installations are very cheap now*" (Main Entrepreneur, February 2018).

How unstable and unreliable affiliate marketing programs related to Android applications are was also mentioned often in the discussions. For example, the Main Entrepreneur said: "*I have no doubt in you (smiley face), but billing and operators are not reliable"* (Main Entrepreneur, August 2017) to someone who hoped that the current

business would last. Similarly, Website Master 1 said: "*Well, nothing you can do. You should always be prepared. This business is not stable"* (Website Master 1, October 2017), meaning that one has to be always prepared for months without income. Similarly, when the Main Entrepreneur asked an affiliate marketer about a program, the latter replied: "*Not yet. The monetization is not stable*" (Affiliate Marketer 1, November 2017) adding the precision that "*not every operator is working right now*" (Affiliate Marketer 1).

Payments from affiliate marketing programs also seem to be volatile. Throughout the conversations, they are often postponed, especially payments related to installations of malicious Geost applications. In fact, the Main Entrepreneur is the middleman between Website Master 1 and those behind the Geost botnet. He is the one transferring money for successful installations to Website Master 1 on their behalf. Questions raised by Website Master 1 as to when payments will be made are frequent, such as, "*Any news about the money?"* (Website Master 1, November 2017) or "*They will not give the money yet?*" (Website Master 1, December 2017) or "*Did they send it [money]?*" (Website Master 1, March 2018). Most of the time, the Main Entrepreneur mentioned that payments were delayed, and eventually the interactions illustrated that the payments had been made. Website Master 1 had to be patient: he had to wait for those behind the program to pay, but also for the Main Entrepreneur to transfer the money. The Main Entrepreneur was also unreliable, often paying Website Master 1 late and apologizing for it: "*Hi, I'm sorry that I have not yet transferred, I was detained [for work] until Sunday, I will immediately transfer 2 payments.*"

The business was so ephemeral that, by the end of the period of study, all programs that the Main Entrepreneur was involved in over the past months had vanished. He thus again asked Affiliate Marketer 1 for business opportunities, mentioning he was just "*Jumping around, looking for something stable* (Main Entrepreneur, March 2018).

Based on these subthemes, the business environment in which these individuals evolved is adverse or, in other words, unpleasant and difficult. No business relationships developed, both in terms of business partners or programs, seem to be fulfilling or efficient and the prospect of making decent money is low. This, coupled with the amateur status presented below, illustrate a rather challenging business context.

7.2. Amateur Work

For the business to be successful, websites have to attract visitors and entice them to download Android applications. To do so, a lot of work must be completed, from website design to content production and visibility. For these reasons, the Main Entrepreneur and his sub-contractors spent a lot of time trying to develop decently performing websites. Based on the discussion surrounding website development and the various difficulties faced, the second theme amateur work emerged from the data. This theme included the subthemes 1) lacking technical skills, and 2) building and working with defective tools, illustrating that the difficulties faced were not resolved by professionals, but rather amateurs. A server hack incident further corroborated this finding, as shown below.

7.2.1. Lacking Technical Skills

Often, when facing technical difficulties, the Main Entrepreneur and his business partners lacked the skills to resolve them efficiently as professionals. The discussions are filled with interventions that illustrate this, such as: "*I am saying I don't know how to split the traffic*" (Main Entrepreneur, November 2017) or "*I cannot understand how to give files from the cache folder*" (Main Entrepreneur, December 2017) and even "*I do not know how to make [use?] the API*" (Main Entrepreneur, December 2017). Similarly, Website Master 1 mentioned: "*I'm not a super programmer either*" (Website Master 1, December 2017) and "*I am not a programmer, I know my files"* (Website Master 1, December 2017). Yet having some programming skills would be useful for individuals developing Android portals for internet marketing purposes.

Moreover, Developer 1 spent a lot of time trying to figure out how to make the websites efficient for search engine optimization purposes; there are hundreds of interactions between Developer 1 and the Main Entrepreneur, where they try to figure out how to set up various techniques to optimize their websites. Yet the end results are not as expected, as Developer 1 one mentioned: "*Our sites are not high-quality, they will not last long*" (Developer 1, December 2017). The Main Entrepreneur tried to convince Developer 1 to continue, arguing: "*Let's make a couple of sites, modify the rest if it doesn't work in a couple of months we'll give up or sell*" (Main Entrepreneur, January 2018).

7.2.2. Building and Working with Defective Tools

The tools used and developed for the business were also flawed and required constant maintenance. For example, hundreds of conversations were focused on fixing a tool called “a parser” that crawls other Android websites to automatically fill the Main Entrepreneur’s website with new content. Yet the tool works badly and is often broken, with the Main Entrepreneur asking Developer 1 to look at it: “*Can you check parser for [website domain name]? It does not parse many categories*” (Main Entrepreneur, November 2017) or “*Parser does not work*” (Main Entrepreneur, November 2017) or “*Hi, fix the parsers as you can, otherwise it’s not good […] (smiley)*” (Main Entrepreneur, March 2018). It is unclear why the “parser” is always broken, but it is clear that they are having problems, with many interventions aimed at fixing it.

Some applications that the Main Entrepreneur advertised on his website for monetization were also flawed, as he mentioned: “*Before the application was getting flagged and did not bring a good conversion rate*” (Main Entrepreneur, October 2017).

Hacking Incident

During the period of study, the Main Entrepreneur’s server was hacked, requiring him to shut down his entire operation and hire someone to clean the server. He mentioned: “*I need to clean up the server and websites from malicious code and programs.*” (Main Entrepreneur, November 2017) when hiring the individual. The hack happened, according to the Main Entrepreneur, because he allowed a friend to host a website and that friend shared the server’s password publicly, leading the server to be hacked and leveraged to send spam and junk links. The Main Entrepreneur thus had to hire someone to help him clean the server. The server cleaner worked tirelessly, and the job took much more time than expected. As the conversation goes on, it becomes clear that the way the server was set up is unprofessional. The server cleaner mentioned: *“[…] Now you have all sites on one server user, you need to create a separate user for each site. Also, each database from the site must be under its own user […]*” (Server Cleaner 1, November 2017) and then stated: “*I went to sleep, your sites exhausted me*” (Server Cleaner 1, November 2017).

Three days later, one of the Main Entrepreneur’s websites was hacked again so he restored the backup files, yet the website was still infected. Not knowing what to do,

the Main Entrepreneur asked for help again from the server cleaner. The server cleaner looked at the set up and noticed, again, unsecure settings. He mentioned: "*In order for the protection to be effective, as well as to prevent reinfection, you need to set secure PHP settings.[…]"* (Server Cleaner 1, December 2017) and "*Now what needs to be done is to restore the site from a clean backup, re-update and set the settings*" (Server Cleaner 1, December 2017). This server hacking incident shows that the Main Entrepreneur might not have been aware of good security measures and practices for the business he was involved in, making him a novice in the field. Overall, the core group of individuals in the private chat log (Main Entrepreneur, Website Master 1 and Developer 1) seemed to lack the required knowledge to conduct their business professionally and efficiently.

7.3. Leniency Towards Criminality

That some of these individuals were involved in criminality was not obvious throughout the conversations, apart from the technical information shared about the Geost botnet. No one talked about spreading banking Trojans or contributing to a botnet. Instead, there were hints that showed that at least the Main Entrepreneur and his two closest business partners were aware that the applications were malicious. Such interactions were grouped in the third theme leniency towards criminality, including 1) shady activities and 2) fighting security measure subthemes.

7.3.1. Shady Activities

At least the Main Entrepreneur and his two closest business partners were aware that they were manipulating malicious applications. For example, when talking about them, the Main Entrepreneur said: "*I see the dangerous file"* (Main Entrepreneur, November 2017). The Main Entrepreneur also talked with Website Master 1 and Developer 1 about an antivirus company blocking the malicious application and developed tactics to "clean" the file (also called "crypting", which basically means obfuscating its code).

Other interventions indicated lenient attitudes towards malicious or shady activities by individuals in the chat log. For example, in a conversation about the potential profitability of a program, Affiliate Marketer 2 mentioned: "*Conversion rate is*

different, but there is no guarantee that total sum will be better than from legal" (Affiliate Marketer 2, November 2017) to the Main Entrepreneur, thus making a distinction between legal and non-legal business opportunities. In another conversation, the Main Entrepreneur asked the money exchanger to be -most likely- a money mule: "*Hi, are you here? I have a proposal for you. Are you interested in these sorts of deals, you give cash, and the customer will transfer money to a bank account + 7%?"* (Main Entrepreneur, January 2018). The offer was refused, yet the conversation between the two continued, as the Main Entrepreneur acted as a middleman for a group that needed to transfer large amounts of money. Based on the conversation, the money exchanger asked a percentage fee (between 10 and 15%) for every exchange while the Main Entrepreneur asked, on behalf of another group, for cash transfers to accounts in China or Bitcoin transfers. The conversation between the two does not indicate whether the deals discussed took place, as there was disagreement about the percentage fees. Given the percentage fees and the transfer methods, there was little doubt -from a reader's perspective- that the money exchanged came from shady proceedings.

7.3.2. Fighting Security Measures

The entrepreneur's websites are also often banned by Google or Yandex Search Engines, illustrating that the activities he is involved in may be considered suspicious from the point of view of legitimate search engine companies. However, whether they are banned because of the way the Main Entrepreneur attempts to gain visibility, such as via purchasing links or SEO campaigns, or because some of the applications hosted on the websites are malicious, was unclear. For example, when talking about his websites in Fall 2017, the Main Entrepreneur mentioned: "*Damn it my tags were not removed yet*" (Main Entrepreneur, October 2017) meaning that some websites are still blocked by the Google or Yahoo search engines. While talking to Website Master 1, the Main Entrepreneur said: "*I still have tags on mine*" (Main Entrepreneur, October 2017) to which Website Master 1 answered: "*Well Yandex can keep them for a long time*" (Website Master 1, October 2017). These bans seemed to be recurrent as even in March 2018, when the Main Entrepreneur talked about the number of installations he had succeeded with, he mentioned 200 installations, and then said: "*With Yandex browser [and no ban], would be 40% more, but alas*" (Main Entrepreneur, March 2018).

Moreover, applications that are "*cleaned*" by being "*crypted*", means that they are obfuscated to avoid detection by antivirus engines. The Main Entrepreneur took several steps to "*clean*" the Geost applications that were on his websites, as they were constantly flagged by antivirus engines as malicious, thus preventing the installation of the application on users' devices. Such work seemed to be redundant and relentless, as shown in the conversation below between the Main Entrepreneur and Website Master 1:

"20:49 – Main Entrepreneur: [file name] the file, right?
20:50 – Website Master 1: Yes
20:51 – Main Entrepreneur: Try to re-crypt. and install.
21:17 – Website Master 1: Done
21:26 – Main Entrepreneur: And again, change file. Re-deploy.
21:49 – Website Master 1: Re-deployed"

Within an hour, the Main Entrepreneur and Website Master 1 had to change the malicious application file on their websites because it had been detected. Such conversations between the Main Entrepreneur and Website Master 1 were recurrent throughout Fall 2017: they constantly needed to re-crypt and re-deploy new malicious applications sent by those behind the Geost botnet. Such relentless and redundant work was highlighted again when the Main Entrepreneur was trying to convince Website Master 2 to spread Geost applications and Website Master 2 answered: "*Too much to deal with*" (Website Master 2, October 2017). These findings spark the questions: why were they involved in such work? What were their motivations?

7.3.3. Seeking Economic Independence

The fourth theme encompassesed what seemed to drive the individuals studied: seeking economic independence. However, whether such a motivation was fulfilled is doubtful: the potential revenue estimated for a website master is much lower than the expected revenue, as presented in the following subsection.

The motivation behind all these activities seemed to be money, as seen in interventions such as: *"Hi, it's time to work. The year has begun. Need to earn money this year"* (Main Entrepreneur, January 2018) or "*Hi, maybe we can still do what we agreed on? A few websites would be enough for the beginning. And it is not that much to do. At the end of the month when we finish, I will get a good payment.*" (Main Entrepreneur, October 2017). Distributing Geost applications seemed to represent an opportunity that could satisfy the Main Entrepreneur's motivations. Indeed, when the

developer did not want to work, the Main Entrepreneur was willing to pay double to motivate him: "*I will pay you double*" (Main Entrepreneur, October 2017) illustrating that the opportunity may have been interesting enough to increase the developer's salary. When the Main Entrepreneur talked to Website Master 2 about an opportunity to distribute Geost applications and Website Master 2 refused, the Main Entrepreneur replied: "*Why don't you want to send this traffic? it is more profitable!"* (Main Entrepreneur, October 2017). Thus, there seems to be a premium profit in spreading malicious applications.

The idea of independence, of not working for someone else (such as a boss), also seemed to be a motivation shared by the Main Entrepreneur and Developer 1. In their conversation, the main entrepreneur tried to convince Developer 1 to continue the work he had started, motivating him with the idea of *money* and *not working for someone else* (as opposed to short-term contracts that Developer 1 does in partnership with the Main Entrepreneur). For example, the Main Entrepreneur mentioned:

> "[…] Look at all pros and cons. The motivation we have is not working for another boss (not to work for someone else). At the end of the month, I will pay you a good amount of money. Also, a motivation. Honestly, let's do it, create a few websites and that's it, then you can relax, and the rest of the work would be on me. *Please understand it is important. And it's not an option to look for another programmer*." (Main Entrepreneur, October 2017).

As Developer 1 stopped working, being discouraged, the Main Entrepreneur continued to try to motivate him, mentioning:

> "Ok, it doesn't go this way. You need to pull yourself together and work. Otherwise, we will continue to work for someone else. And make money for other people. Seriously, you need to gather your strength and start to work, moreover I already started buying links for our domains" (Main entrepreneur, October 2017).

In this statement, the Main Entrepreneur mentioned a wish to stop working for someone else. Yet Developer 1 was discouraged by their business, which seemed to yield little profit, not providing him with the recurrent income he was expecting: "*The fact is, I already did several times some stuffs for passive income, and then did nothing. And passive income is gone."* (Developer 1, November 2017) and "*Yes, I don't see any prospects, I realized that I was led by the fact that others make good money […]* (Developer 1, January 2018). Passive income refers to developing a business that would

pay regularly afterwards with little effort. In the previous statement, Developer 1 mentioned that he was led by the idea that others were making good money, thinking that he could achieve such economic independence as well.

Success?

The conversation between the Main Entrepreneur and Website Master 1 yielded insights into the potential revenue that can be achieved by a website master when distributing malicious applications. This is because Website Master 1 distributed Geost applications on his own websites (just like the Main Entrepreneur) and for every successful installation, the Main Entrepreneur transferred money to Website Master 1 on behalf of those behind the Geost applications.

Potential revenues were estimated by considering every time the Main Entrepreneur sent money to Website Master 1 with mentions such as: "*Money was transferred"* for *"[number] of installs*". For example, the Main Entrepreneur said once: "*Transfer for 200 [installations], check it please*" (Main Entrepreneur, November 2017), to which Website Master 1 replied: "*How much is this one now?*" (Website Master, November 2017) and the Main Entrepreneur replied: *"Four thousand, with commissions 3700*" (Main Entrepreneur, November 2017). The interventions indicated that Website Master 1 was paid 18.5 rubles (3,700 rubles / 200 installed applications) per malicious applications installed. The commission fees are exchange fees charged by the online payment service QIWI, a payment service used by Russian citizens. Another example would be: "*Hi, 9k transferred check*" followed by "*For 500"* (Main Entrepreneur, January 2018), which meant, in this case, 18 rubles per malicious application.

The potential revenue of Website Master 1 was thus calculated by considering all payment mentions like those presented above. When only the number of installations was mentioned, the latest price per application (in the conversation) was considered, which ranged between 17 and 20 rubles. Transferred payments found in the conversation are presented in Table 3, along with the date.

Table 3 Business Partners related to the Main Entrepreneur

	Installation	Price per application	Rubles
2017-10-04	250	20	5000
2017-10-16	437	20	8740
2017-10-20	350	20	7000
2017-11-05	700	18.57	13000
2017-11-13	410	18.57	7600
2017-11-18	200	18.57	3700
2017-11-30	325	18.57	6000
2017-12-06	444	18.01	8000
2017-12-22	666	18.01	12000
2017-12-27	555	18.01	10000
2017-12-29	333	18.01	6000
2018-01-07	555	18.01	10000
2018-01-10	500	18	9000
2018-01-20	666	18.02	12000
2018-01-29	102	17.65	1800
2018-02-02	278	17.99	5000
2018-02-19	56	17.86	1000
Total	**6,827**		**125,840**

Website Master 1 thus made an estimated potential revenue of 125,840 rubles (~USD 2,157.38[17]) for 139 days (from October 2017 to February 2018) due to 6,827 devices installing the malicious application Geost. This represents 6,827 potential victims during near five months. Whether such an amount is substantial depends on one's perspective. Yet this revenue may not be exactly what these individuals were expecting: when the Main Entrepreneur was talking about other opportunities that could pay, he mentioned that "*Movie sites can collect 20 thousand [rubles] per day*" (Main Entrepreneur, November 2017). Over the 139 days of operation investigated above, this would represent a revenue of 2,780,000 rubles (USD 47,659.86), more than 2,000 times what Website Master 1 made with the Geost applications.

[17] The exchange rate as of December 31st, 2017 was considered, which was 58.33 rubles for one US dollar.

7.4. Indispensable Workers Dancing on the Crime Line

The above analysis uncovered the challenges and motivations of individuals involved in spreading malicious Android applications related to the Geost botnet. They were, in the end, amateurs with leniency towards criminality and motivated by economic independence but facing an adverse environment. By taking a step back from the analysis, one may notice that, in the end, the Main Entrepreneur and his business partners were not the motivated offenders behind the Geost botnet, but rather the **indispensable workers** mentioned by experts in the interviews.

They were those positioned at the periphery of criminal organizations, doing the licit tasks, such as building websites. For this specific scheme, Geost operators (the minds behind the botnet scheme) needed these workers to spread the malicious applications. Indeed, through the work of these indispensable workers, banking Trojan applications were made available on Android portals and downloaded by individuals. These individuals, with their leniency towards criminality, ended up participating in the scheme, lured by potential profits. However, the profits made were not as high as their expectations.

7.5. Uncovering an IT Informal Workforce

These findings yield insights on the actors positioned at the periphery of online economic crime organizations. However, is there a way to expand the analysis through *quantitative* lenses and assess the extent to which such leniency towards criminality is generalized? Do individuals from the IT sector, like the individuals studied above, tend to participate in online economic crime easily and quickly for the lure of profits?

These inquiries are explored in the second part of this thesis, thanks to information in the private chat log that pointed towards a digital labor platform specialized in IT services. Indeed, three individuals, namely, the Main Entrepreneur, Website Master 1 and Developer 1, also discussed their business on such a platform. The association was possible because 1) links to specific posts on the public platform were shared within the private conversations (e.g., "*ordered texts [link to comment on the public platform*]" (Main Entrepreneur, January 2018) and 2) these three individuals used the same usernames in the private chat log as in the public platform.

The platform is named searchengines[dot]guru and is a Russian- and English-speaking platform dedicated to Internet marketing. It appeared in early 2000 and, as of 2021, reported over 400,000 registered members and 14,000,000 comments. The platform advertises itself as a "*website allowing users to discuss issues related to creating and promoting websites on the Internet*". It is divided into categories that cover various aspects of internet marketing, allowing the matching of labor supply and labor demand on specific aspects surrounding the business.

However, because the platform advertises itself as a place where individuals can *discuss* issues related to creating and developing websites, and not as a "matchmaker" for labor demand and supply, it is less organized or formal than digital labor platforms (e.g., freelancer platforms) mentioned in previous research. These digital platforms are already known as unregulated spaces where informal work is thriving (Schmidt, 2017; Drahokoupil and Piasna, 2017; Drahokoupil and Fabo, 2016).

In this thesis, this platform is conceptualized as a platform gathering informal workers specialized in IT services. These are *workers* because internet marketing involves business-related activities, and most users use the platform to offer and demand various cloud work. They are *informal* workers because most (not all) economic activities, happening through the platform, are most likely unregulated or unregistered, similar to *formal* digital labor platforms (Schmidt, 2017; Drahokoupil and Piasna, 2017; Drahokoupil and Fabo, 2016) .

The remainder of this thesis focuses on assessing this informal IT workforce's potential ties with criminal spaces. **For now, searchengine[dot]guru is referred to as an (the) informal platform since it gathers both discussions about and sales of IT-related products and services.**

Chapter 8.

Methods for Drifters and Non-Drifters Comparison

The second part of this thesis takes a quantitative approach to assess the uncovered informal IT workforce's potential availability to participate in online economic crime tasks. This is done by evaluating informal workers' commenting patterns between the informal platform and crime-oriented ones. Crime-oriented platforms are platforms that embody a criminal ethos, such as carding or black hat SEO. To differentiate workers who talked on crime-oriented platforms, the concept of **drifter** is developed. Drifters are individuals from the uncovered informal IT workforce that discussed, at least once, in a crime-oriented platform.

The second objective of this study is to assess drifters' relationship between informal and crime-oriented spaces. To fulfill this objective, whether drifters formed a distinct group that could be identified on the informal space is first assessed. If so, then the drifters' distinctive group would require further investigation. The research question that leads the following analyses is: *"Does drifters' behavior on the platform differ from that of non-drifters?"*

The chapter presents the methodological strategy developed to answer this question. First, the data creation process and validation are presented. This includes creating a dataset of the workforce, finding other platforms on which the workforce discussed, identifying whether these platforms are "crime-oriented", and dividing the workforce between drifters and non-drifters. Second, the four indicators developed to grasp workers' behavior on the informal platform are outlined, namely, activity rate, diversification level, business purposes, and specialized topics. Third, the comparison strategy, which includes a series of Mann-Whitney U tests, is explained.

8.1. Dataset Extraction

Gathering a dataset including the informal workforce and its potential ties to other crime-oriented platforms was made possible by an academic access to the Flare

Systems[18] portal and its application programming interface (API). Flare Systems is a Montreal-based company that has developed a digital risk protection and cyber threat intelligence platform. It has been monitoring the informal platform as well as over 100 other online platforms over the past years. For the informal platform[19], it has collected more than 12,000,000 comments, some of these comments dating back to early 2000. The academic access to Flare Systems was first used to create the informal workforce dataset. To begin, I ensured that Flare Systems had a valid assessment of the informal platform. To do so, fifty random actors were selected, and the number of comments found on the Flare Systems database was compared to the number of comments found on the platform from 2012 to 2020[20]. Based on this random sample of actors, Flare Systems had, on average, 93% (std=0.13) of the total number of comments published on the platform, illustrating that it had a relatively good visibility.

The private chat log discussions took place in 2017 and 2018 and the three individuals involved in malicious activities, the Main Entrepreneur, Website Master 1 and Developer 1, also discussed on the informal platform during these years. To be as close as possible to the economic context uncovered in the private chat log, these two years served as a ground point for the following analysis on the informal platform.

Using the Flare Systems API, all comments posted on the informal platform in 2017 and 2018 were extracted. For each comment, the comment's identification number, text, timestamp, and the name of the actor who wrote it were extracted, along with the title of the thread in which it was posted and the thread's identification number. One actor's name was "Этот пользователь удален," which means "This user has been deleted". Consequently, all comments related to this specific actor's name were

[18] https://flare.systems/

[19] Searchengines[dot]guru is called the "informal platform" for the remainder of this thesis.

[20] The time-period 2012-2020 was selected because the platform was revamped in June 2020 (see Valeros and Garcia, forthcoming) and the number of comments published on the platform before 2012 was incomplete. For example, for the 50 actors investigated, the informal platform listed their comments from 2012 to 2020, and then a few comments in 2009 and 2010, and almost no comments from 2000 to 2009. On the other hand, comments dating back to early 2000 were available in the Flare Systems database, illustrating that the "revamping" of the platform may have resulted in a loss of information. This was further confirmed when some mismatches were found between the Flare Systems database and the informal platform: Flare Systems had more information than did the informal platform on each actor. When assessing Flare's visibility, only situations where the number of comments on Flare was lower than or equal to what was published on the informal platform were considered, resulting in a high visibility of 93%.

removed. A total of 685,815 comments, 34,706 threads and 23,348 individual users were extracted.

The dataset was augmented with the thread's category and subcategory as displayed on the website. Using the thread identification number, the thread's category and subcategory were extracted from the source code of the page using an automated web crawler. Such crawling was achieved over several days to ensure that the platform's server would not experience disruption from the research activity. A total of nine categories and 80 subcategories were found. Table 4 shows the nine categories and a sample of their subcategories. Topics ranged from questions about search engine optimization to hiring webmasters to monetizing websites. Table 4 also illustrates the distribution of comments across categories. The category "about monetizing sites" was the most popular one, representing 20% of the comments, followed by "not about work" with 17% and site building with 16%.

Table 4 Categories and Subcategories on the Informal Platform

	Category	Subcategory	% of Comments
1	Search Engine	Yandex, Site Directories, Google	10%
2	About Monetizing Sites	Partnership Programs, General Questions about Making Money on Sites, YouTube Monetization	20%
3	Practical Optimization Issues	Popular SEO and SEO Newbie Questions, Doorways and Cloaking, General optimization issues	13%
4	Communication of Professionals	Cryptocurrencies, Ecommerce, Social Media Marketing	14%
5	Site Building	Domain Names, Hosting and Servers for Websites, Web Analytics, Copywriting	16%
6	Exchange and Sales	Buying and Selling Sites, Digital Goods, Programs and Scripts	5%
7	About Purchased Traffic for Websites	Teaser and Banner Advertising, Contextual Advertising, Yandex Direct, Google Ads	2%
8	Work and Services for Webmasters	Copywriting Translations, Social Media Marketing Services, Optimization Promotion and Audit	3%
9	Not About Work	Meetings and Gatherings, Smoking Room, About the Site and Forum	17%

8.2. Sample Description

Based on the above dataset, Table 5 presents the descriptive statistics on users' participation in terms of the number of comments they posted on the platform as well as the number of threads and categories in which they participated. In 2017 and 2018, users commented, on average, 29 times (std=151) on the platform, with a minimum of one, a median of four, and a maximum of 6,603 comments. This maximum represents, posting, on average, nine times per day over a two-year time span. A major contributor could credibly have such posting behavior. Thus, all users in the end-tail of the posting distribution were kept for the analysis. Also, users participated, on average, in eleven threads (std=50), with a minimum of one thread and a maximum of 2,013 threads. Half participated in two or fewer threads. In terms of categories, users posted, on average, in two categories (std=2), with a minimum of one and a maximum of nine. Half participated in only one category.

Overall, according to these statistics, user participation was unequal, with most users exhibiting a low rate of participation. This skewed distribution reflects the participation inequality rule found in online communities and highlighted by scholars (Haklay, 2016; Paquet-Clouston, Décary-Hétu and Morselli, 2016; Sun, Rau, and Ma, 2014; van Mierlo 2014; Mooney and Corcoran 2012; Lund, Coulton, Wilson, 2011; Budhathoki, 2010). Among the most well-known distributions is the 90-9-1 law formulated by Nielsen (2006): 90% of users in online platforms are lurkers who do not contribute; 9% are intermittent contributors; and 1% are heavy contributors. Thus, in most online platforms, only a small proportion of users contribute to most of the content, while silent and minor contributors form the great majority of users (Haklay, 2016; Sun, Rau, and Ma, 2014,).

In the current dataset, the large number of minor contributors may significantly impact the analysis, driving indicators closer to zero (e.g., total number of comments). For this reason, a subsample was created to consider only the proportion of the population at the end-tail of the distribution. In the distribution of comments per user, there is a slight breakdown at 10 comments, with about 70% of users posting fewer than ten comments and 30% posting more than ten comments, as shown in Figure 4 (which includes users who posted less than 100 comments).

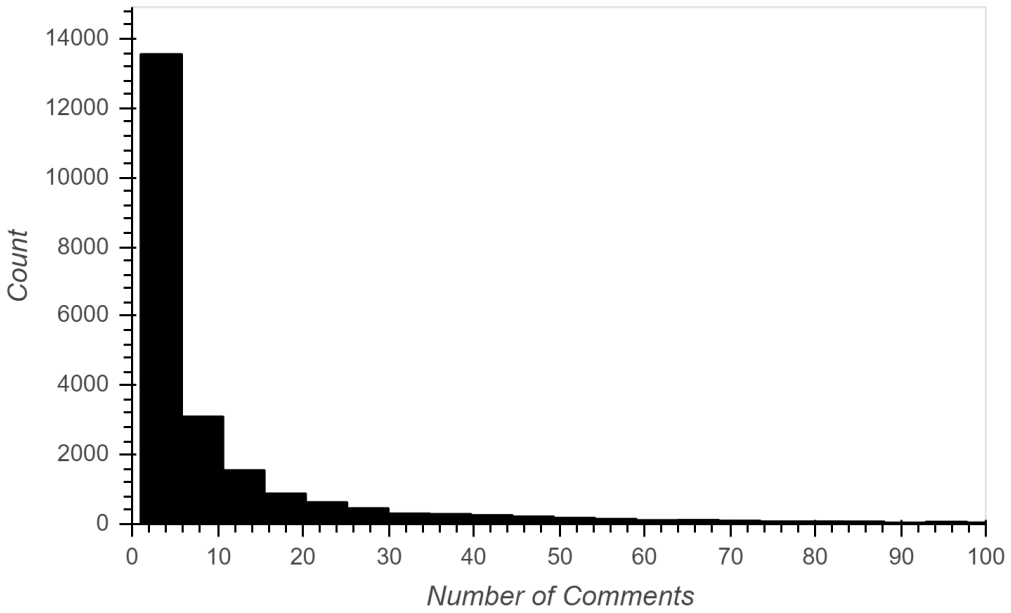

Figure 4 Distribution of Comments for Users who Posted Fewer than 100 Comments on the Informal Platform

Given this distribution, a subsample was created including only users who posted at least 10 times in 2017 and 2018, representing the top 30% (N=6,924). Table 5 also presents the descriptive statistics on user participation for this top 30%. In this subsample, users are more active: they posted, on average, 92 comments (std=267), with a minimum of ten and a maximum of 6,603. Users also posted in, on average, 34 distinct threads (std=88) and, on average, four categories (std=2).

Table 5 Descriptive Statistics on the 2017-2018 Dataset

	Min	Max	Mean (std)	Med
All Dataset N= 23,348 users				
N. Comments	1	6,603	30 (151)	4
N. threads	1	2,013	11 (50)	2
N. Category	1	9	2 (2)	1
Top 30% N= 6,924 *users*				
N. Comments	10	6,603	92 (267)	27
N. threads	1	2,013	34 (88)	12
N. Category	1	9	4 (2)	3

8.3. Identifying Drifters

Drifters in this study are individuals who comment on the informal platform and at least once on a crime-oriented platform, such as a hacking forum. Given that users pick usernames to identify themselves in online communities, identifying drifters is possible by cross-correlating usernames on different platforms. The assumption behind cross-correlating usernames is that users may chose the same username -or a similar one- across platforms, a behavior identified in previous studies (Wang et al., 2016; Perito et al., 2011). Indeed, Wang et al. (2016) and Perito et al., (2011) correlated similar usernames across platforms and could identify real-world individuals. Given that the most efficient way to identify individuals across platforms is through their usernames, such a strategy is taken to identify drifters.

The Flare Systems portal and application programming interface (API) allowed searching for the name of an actor and finding other platforms on which the actor engaged. Thus, considering the dataset that included all individuals who spoke on the informal forum in 2017 and 2018, a list of usernames was created. Each of these usernames could be queried on the Flare Systems database using a perfect math approach: if the username were found to have commented on a platform other than the informal one, then Flare's identification number for the comment, its timestamp, and the name of the platform on which it was posted could be extracted and added to a separate dataset. However, before querying Flare Systems' database, filtering processes were developed, as explained below.

8.3.1. Filtering Processes

Two filtering processes were developed: one considering username length and sophistication, and a second one considering the timestamp of comments posted outside the informal platform. Both processes are explained below.

Username Filters

To minimize the chances of cross-correlating usernames that could belong to different individuals due to the popularity or lack of sophistication of the usernames, three filters were developed. The first filter, the base filter, considered only usernames formed of at least five characters, thus removing several common usernames such as

“Nick”, “Max,” or “bot,” as well as two, three or four-letter usernames. Although some of these usernames could be quite sophisticated, an investigation of the list of such short usernames indicated that there were plenty of generic ones that could be removed by applying this minimal filter. The base filter reduced the number of users (eligible to be drifters) to 21,726.

The second filter considered only usernames with at least 6 characters, reducing the number of potential individuals to 19,291. The third filter considered usernames with at least 5 characters AND at least an uppercase OR a number OR one special character, leading to 14,863 potential individuals. Note that none of these filters is better than the others. Filters 1 and 2 are more liberal, but they are likely to include generic usernames. Filter 3 is more conservative but is also likely to dismiss individual usernames with only lower-case characters. Finally, they are all likely to dismiss false negatives like usernames with fewer than five characters but with four uniquely ordered ones. The idea is to minimize the chances of cross-correlating generic usernames and maximizing the chances of keeping one-of-a-kind usernames[21].

Thus, based on this filtering process, all usernames with at least five characters (N=21,726) were searched for in the Flare Systems database and a separate dataset was created including all drifters. This database included (1) Flare’s identification number for the comment, (2) its timestamp, (3) the name of the platform on which it was posted, and (4) the related username.

Timeframe Filters

Flare Systems has strong visibility on other platforms, and some of these platforms have been active since early 2000. Thus, once the drifter dataset was created, additional time filters were developed to prevent identifying a user who posted on another platform in 2005 as the same user who posted on the informal platform 12 years later due to the same username. For the filters to be accurate, they had to isolate comments posted around 2017 and 2018. To make sure that the results were not an artefact of the filtering decisions, three filters with different timeframes were developed.

[21] Individuals impersonating other individuals (doing username mimicry) could also yield false positives. However, there are no reasons to believe that username mimicry is a concerning phenomenon within the informal platform population.

The first filter (2015-2020), the most liberal one, considered all comments posted on other platforms two years prior to 2017 and two years after 2018, that is, from 2015 to 2020. The second filter (2017-2019) considered all comments posted on other platforms one year prior to 2017 and one year after 2018, thus from 2016 to 2019. The third filter (2017-2018), the most conservative one, considered only comments posted on other forums during the period of study: in 2017 and 2018. These filters aimed at minimizing the chances of cross-correlating usernames that might not belong to the same individuals because of the time difference between the comments posted, while also generating a sufficient dataset for the analysis.

8.3.2. Confirming the General Purpose of Crime-Oriented Platforms

Before presenting the drifter dataset, an additional step was required as I had to investigate whether the platforms on which drifters discussed were crime-oriented, displaying a clear association with criminality in the platform's branding[22]. A total of 42 external platforms were found and **each of them was visited to categorize its general purpose**. Sometimes, the platforms were down (which is frequent for those hosted on the Tor network) or required registration. In such cases, to find their general purpose, security reports and blogs about them were searched for on the general web or information from the Flare System database was used.

Four platforms were **not** identified as "crime-oriented". They rather focused on technological topics such as cybersecurity. They were thus removed. On the other hand, the remaining **38 platforms** were openly related to criminal activities. Of these, 17 were hosted on the "clearnet", meaning that they could be visited via a modern web browser such as Google. The remaining 21 were hosted on The Onion Router (Tor), known as part of the "darknet".

Tor is an anonymous communication protocol developed by a network of volunteers that allows users to browse the internet anonymously[23]. The anonymous protocol also hosts websites, known as onion services, that offer anonymity to both website owners and visitors. These onion services are often associated with the "darknet

[22] The term platform is used throughout this thesis. It is a generic term to refer to websites where individuals can discuss and/or sell products and services.

[23] https://www.torproject.org/

(Fidalgo et al., 2019; Broadhurst et al., 2020; Owen and Savage, 2015), a loosely defined concept that encompasses networks that are not accessible via modern web browsers and offer anonymity to their users, such as I2P, Freenet, Tor, and ZeroNet (Hu, 2020). Content is more likely to be related to criminal activities when hosted on these technologies due to the anonymity provided[24].

8.3.3. Drifter Dataset

Following this last cleanup, nine (sub)datasets were created by combining the username filters with the time filters. These nine (sub)datasets were further subdivided into (1) the whole population and (2) the top 30%. Thus, the number of drifters and external platforms found varied depending on the filters and the population considered, as shown in Table 6.

Table 6 Drifters Identified Based on the Combined Filters for the Whole Dataset and the Top 30%

	2015-2020				2016-2019				2017-2018			
	Dataset		Top 30%		Dataset		Top 30%		Dataset		Top 30%	
	Drifters	*Plat.*	*Drifters*	*Plat.*	*Drifters*	*Plat.*	*Drifters*	*Plat.*	*Drifters*	*Plat.*	*Drifters*	*Plat.*
Min 5 chars	1,557	38	510	31	1,160	34	379	30	696	31	231	25
Min 6 chars	1,234	38	395	30	924	34	290	29	557	31	177	24
Min 5 chars +	946	36	330	28	700	32	244	28	421	30	152	23

Combining the most liberal filters (username length: min 5 chars and timeframe: 2015-2010) led to finding 1,557 drifters posting on 38 crime-oriented platforms for the whole population and 510 drifters posting on 31 external platforms for the top 30%. On the other hand, combining the most conservative filters (username length: min 5 chars+ and timeframe: 2017-2018) yielded 421 drifters on 30 platforms for the entire population and 152 drifters on 23 platforms for the top 30%. Overall, drifter datasets vary from 421

[24] However, whether the content available on onion services is solely criminal is subject to debate. For example, Faizan and Khan (2019) found that 66% of the content hosted on these websites was licit while Owen and Savage (2015) reported that the majority of the content hosted on the network was related to crime.

to 1,557 for the whole population and from 152 to 510 for the top 30%, depending on the combination of filters used.

8.4. Behavior Indicators

To assess whether drifters and non-drifters behaved differently on the informal platform, four indicators were developed for each actor: (1) activity rate, (2) diversification level, (3) potential business interactions, and (4) topics discussed. Each contains various sub-indicators as explained below.

8.4.1. Activity Rate

Activity rate assessed whether drifters were more active on the informal platforms than on the crime-oriented platforms. It was measured through two sub-indicators: (1) the sum of all comments made by a user in 2017 and 2018 and (2) the number of days an individual was active over the two-year period, meaning the number of days an individual posted at least once.

8.4.2. Diversification Level

The diversification level assessed whether drifters were more diversified in terms of topics discussed on the informal platform. This level was measured through three sub-indicators. First, the Standard Diversity Index (SDI) developed by Agresti and Agresti (1978) was calculated, as expressed in eq. (1),

$$SDI = \left[\frac{k}{1-k}\right] 1 - \sum_{i=1}^{k} p_i^2 \text{ eq. (1)}$$

where k represents the number of categories and P_i the proportion of observations in the ith category where $i = 1 \ldots k$. Thus, the index shows if an actor posts, on average, in several categories or only one category. More precisely, it calculates what is the probability that two comments picked randomly (from the same individual) will be from the same category. The SDI ranges from 0 for no diversity to 1 for perfect diversification. The two remaining sub-indicators for the diversification level were the number of categories and the number of subcategories in which an individual commented.

8.4.3. Potential Business Interactions

This indicator aimed at assessing (roughly) whether drifters talked more about cash and money than non-drifters on the informal platform, hence being more business inclined. It was measured through two sub-indicators: (1) the number of comments in which an individual mentioned the words “dollar(s)” and/or “ruble(s)” or their respective signs “$” or “₽” and (2) the proportion of comments with a dollar or ruble sign among an individuals’ total number of posts.

8.4.4. Specialized Topics

The last indicator measured whether drifters were specialized in one of the platform’s topics or, in other words, whether drifters talked more (in terms of the number of comments) in any of the nine categories available on the informal platform, than in the others. These categories are listed in Table 4. They have specific sets of rules enforced by the platform administrators (see Valeros and Garcia, forthcoming).

In short, the **search engines** category includes any discussions related to popular search engines like Yandex or Google. **About monetizing sites** includes discussions on how to make money with websites, with a special focus on affiliate marketing programs. **Optimization practices** includes discussions on website promotions, such as SEO techniques. **Communication of professionals** encompasses topics related to finances and businesses, including money exchanges through electronic payments or cryptocurrencies. The **site building** category is about technologies, solutions, and services associated with building websites, such as virtual hosting or server administration. The **exchange and sales** category focuses on tools, services, and jobs related to internet marketing at large, like the sale of domains or finding skilled workers to develop scripts. **About purchased traffic for websites** includes discussions on advertising campaigns and how to purchase internet traffic. **Work and services for webmasters** encompasses topics on how to efficiently maintain a website, including copywriting, design, and audit services. The last category, **not about work**, contains various unrelated topics such as sports and travels.

For a deep dive into the categories, one can refer to Valeros and Garcia’s forthcoming study on the services exchanged on the informal platform. Overall, each of

these categories has similar purposes such as internet marketing, yet their subtopics are specific, from purchasing internet traffic to building websites to hiring skilled professionals. Measuring whether there are significant differences between drifters and non-drifters in terms of the number of comments in each of these categories will illustrate whether drifters cluster in specific spaces of the platform.

8.5. Descriptive Statistics on Indicators

The descriptive statistics for each sub-indicator are presented in Table 7 for both the entire platform population (N=23,348) and the top 30% (N=6,924).

Table 7 Descriptive Statistics on Sub-Indicators

	All Dataset N=23,348				Top 30% N=6,924			
	Min	**Max**	**Mean (std)**	**Med**	**Min**	**Max**	**Mean (std)**	**Med**
Activity Rate								
Number of posts	1	6,603	29 (151)	4	10	6,603	92 (267)	27
Number of days active	1	708	14 (41)	3	1	708	41 (67)	17
Diversification								
SDI	0	1	0.3 (0.4)	0	0	1	0.5 (0.4)	0.6
Number of categories	1	9	2 (2)	1	1	9	4 (2)	3
Number of sub-categories	1	71	3 (5)	1	1	71	7 (9)	4
Business								
Number of $ in comments	0	1,225	1 (11)	0	0	1,225	3 (20)	0
Proportion of $ comments	0	1	0.04 (0.1)	0	0	1	0.04 (0.1)	0
Topics Discussed								
Search Engines	0	1,109	3 (21)	0	0	1,109	9 (38)	0
About Monetizing Sites	0	3,010	6 (42)	0	0	3,010	18 (75)	1
Practical Optimization Issues	0	2,965	4 (31)	0	0	2,965	12 (56)	1
Communication of Professionals	0	2,363	4 (41)	0	0	2,363	13 (75)	0
Site Building	0	2,873	5 (45)	0	0	2,873	14 (81)	1
Exchange and Sales	0	689	2 (10)	0	0	689	4 (17)	0
About Purchased Traffic for Websites	0	880	1 (10)	0	0	880	2 (18)	0
Work and Services for Webmasters	0	296	1 (6)	0	0	296	3 (11)	0
Not About Work	0	3,532	5 (71)	0	0	3,532	16 (129)	0

As shown in Table 7 when considering the entire population, individuals have posted on average and over two years 29 comments (std=151) on the informal platform,

with a minimum of one and a maximum of 6,603, and they have been active, on average, 14 days (std=41). In terms of diversification within their own posting patterns, individuals are not diversified (mean=0.3, std=0.4). On average, they post in two categories (std=2) and in three subcategories (std=5). Moreover, individuals post, on average, one comment with a dollar or ruble sign (std=11), and the average proportion of dollar or ruble signs in the pool of comments per individual is low (0.04, std=0.1). In terms of topics discussed based on the platform's categorization, the average posting spans from one to six posts with standard deviations going from six to 71. For all categories, at least 50% of individuals do not post at all.

When considering the top 30%, the average participation for each sub-indicator increases. Individuals in the top 30% subsample have posted on average and over two years, 92 comments on the informal platform (std=267), with a minimum of 10 and a maximum of 6,603, and they have been active, on average, 41 days (std=67). In terms of diversification, within their own posting patterns, individuals are relatively diversified (mean=0.5, std=0.4). On average, they post in four categories (std=2) and in seven subcategories (std=9). Moreover, individuals post, on average, three comments with a dollar or ruble sign (std=20) and the average proportion of dollar or ruble signs in the pool of comments per individual is, again, low (0.04, std=0.1). In terms of topics discussed based on the platform's categorization, the average posting spans from two to 18 posts with standard deviations from 11 to 129. For all categories, at least 50% of individuals in the sample do not post at all or have posted only one comment.

8.6. Comparing Drifters and Non-Drifters: Mann-Whitney U Tests

To compare drifters and non-drifters, a series of Mann-Whitney U tests were computed using the behavior sub-indicators developed above. A Mann-Whitney U test was favored over more common parametric tests because all sub-indicators did not follow a normal distribution[25].

Also known as Wilcoxon Rank Sum or Mann-Whitney-Wilcoxon, the Mann-Whitney U test assesses whether the distributions between two groups differ while

[25] This was confirmed by using the normal test function from the scipy.stats package.

making no prior assumptions on the form of the distributions tested (Hart, 2001). The assumptions behind the tests are rather that the data from the two groups are independent, that they follow a similar shape and that they are ordinal or continuous. The datasets used respect such assumptions. The sub-indicators for both drifters and non-drifters are independent (e.g., the posting behavior of drifters is independent of the posting behavior of non-drifters); the distribution shapes of each sub-indicator for both groups are similar (as shown below); and the sub-indicators are ordinal or continuous.

The test compares the two groups by ranking their respective values from low to high and then comparing the ranks between the two groups (Shier, 2004). The number of times a value in group A is greater than a value in group B is counted and the total is known as U_a. The inverse is computed to find U_b. For two identical ranks, half the tie is given to one value and the other half is given to the other tied value during the counting procedure. The resulting statistic U (thus Mann-Whitney U) is the minimum of the two values found: $min(U_a, U_b)$. The lower the U is, the higher the difference between the two distributions is. Also, when U_a is approximately equal to U_b, then the null hypothesis is not rejected and the distributions of the two groups are considered equal. To assess the significance of the test, the Mann-Whitney U uses a z distribution (a standard normal table) when the sample size is greater than 20. The z −score is calculated according to the function presented in eq. (2)

$$z = \frac{U - \frac{N_a - N_b}{2}}{\sqrt{\frac{N_a * N_b\,(N_a + N_b + 1)}{12}}} \quad \text{eq. (2)}$$

where N_a is the sample size of group A, N_b is the sample size of group B, and U is the $min(U_a, U_b)$. If the z-score found is less than -1.96 or greater than 1.96, the null hypothesis is rejected. Given the test's procedure, unbalanced sampling among the two groups is not an issue.

To compute the series of Mann-Whitney U tests, the *mannwhitneyu* function from the ScipyStats package was used[26]. For each sub-indicator, the null hypothesis (H0) was: *there is no difference between drifters and non-drifters*, and the alternative

[26] The test handles for ties, as explained above, and uses a continuity correction.

hypothesis (Ha) was: *there is a difference between drifters and non-drifters*. The significance level of the tests (α) was set to 0.05, meaning there was a 5% risk of concluding that a difference exists when there is no difference. For each group (drifters and non-drifters) and each test, the group's mean, standard deviation, and median are reported, along with the *mannwhitneyu* statistics (U) and the p-value of the test. To report the effect size, the common language effect size, introduced by McGraw and Wong (1992), is used, denoted as f and illustrated in eq. (3)

$$f = \frac{U}{N_a * N_b} \quad \text{eq. (3)}$$

where U is the Mann-Whitney U statistics, N_a is the sample size of group A, and N_b is the sample size of group B. The function f represents the proportion of favorable pairs that support one direction, let's say group A over group B (McGraw and Wong, 1992). The reported U in the scipy.stats package is the $min(U_a, U_b)$, and the f calculated with this U represents the proportion of favorable pairs for the group that has the lower number of favorable pairs. Thus, $1 - f$ is computed below to find the proportion of favorable pairs for the group that has the higher number of favorable pairs. The statistic $1 - f$ is reported, as well, for each test. Thus, for each indicator, $1 - f$ represents the proportion of favorable pairs for the group that scored the highest for that indicator.

Chapter 9. **Indistinguishable Drifters**

This chapter presents the results on whether drifters form a distinctive group within the informal workforce. The research question leading the analysis was: *"Does drifters' behavior on the platform differ from that of non-drifters?"* Based on the behavior indicator developed, they do not.

The chapter starts by briefly presenting the crime-oriented platforms found as well as drifters' posting patterns on them. Then, the Mann-Whitney U tests results are shown for the whole population and the top 30%. A short summary of the main findings concludes the chapter.

9.1. Exploring Crime-Oriented Platforms

A total of 21,726 users on the informal platform had a username with at least five characters. Of these individuals, 7.2% (1,557 individuals) were identified as drifters based on the 2015-2020-time filter, 5.3% (1,160 individuals) considering the 2016-2019-time filter, and 3.2% based on the 2017-2018-time filter (696 individuals). Also, based on the most liberal filtering approach (username of five characters and 2015-2020), a total of 38 crime-oriented platforms were found.

In terms of their general purpose, seven focused on **hacking**; seven were related to **cracking** (cracked software) or **leaked information** (e.g., lists of usernames and passwords); six focused on **carding** (credit card fraud); three were **cryptomarkets** (marketplaces hosted on Tor); one involved **money laundering** discussions; and one was specialized in sharing **blackhat SEO techniques**. Thirteen platforms were hosted on the **darknet** and gathered various discussions and/or sales and/or questions on various content, most often **crime-oriented topics**.

Figure 5 illustrates the distribution of platforms in terms of (1) the platform's accessibility via the clearnet or the darknet, (2) the platform's main identified purpose, (3) the number of drifters who interacted on it, and (4) the total number of comments. The figure is a tree map where the size of the boxes represents the number of drifters in the sample who interacted on the platform (also specified under the platform's name) and the color scale represents the number of posts on each platform. Appendix B also

presents a table with the information, as some platforms have too few actors to be visible in Figure 5.

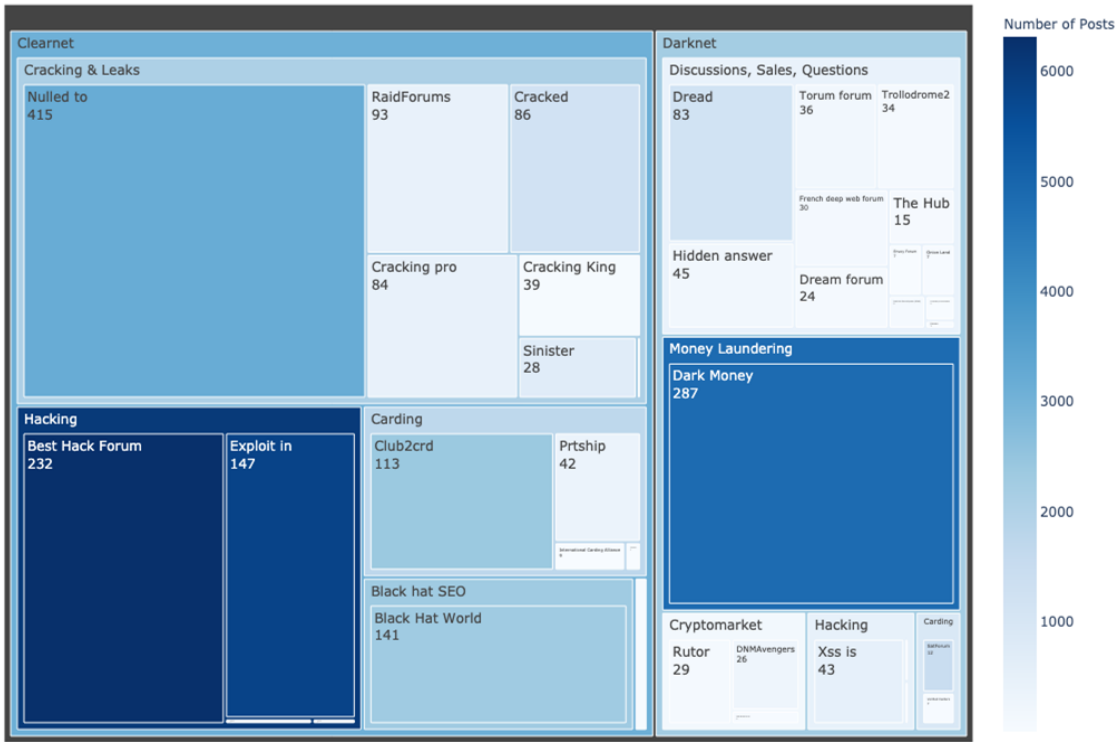

Figure 5 Tree Map of Crime-Oriented Platforms Found

Platforms are grouped by type; the size of the box represents the number of actors (also specified under the platform's name) and the color scale represents the number of posts.

In terms of number of users, the most popular platforms included Nulled.to (cracking and leaks), Dark Money (money laundering), Best Hack Forum (hacking), Exploit In (hacking), Black Hat World (Black Hat SEO), and Club2crd (carding). These crime-oriented platforms are also the ones with the greatest number of posts, although in a different order. Overall, drifters commented on a variety of crime-oriented platforms, from cracking (and leaks) to hacking or money laundering.

Investigating further the data showed that drifters favored crime-oriented platforms hosted on the clearnet over those hosted on the darknet. A total of 67% of drifters' comments were posted on crime-oriented platforms hosted on the clearnet. Moreover, 61% of drifters commented only on clearnet platforms, 25% only on darknet platforms and 14% on both.

To assess drifters' involvement in crime-oriented platforms, their comment frequency was examined. Each drifter posted, on average, 21 comments on crime-oriented platforms (std=75), with a minimum of one and a maximum of 1,383. Also, 50% of drifters posted three comments and 75% posted only ten comments. ne may wonder whether those who commented heavily on the informal platform are the same individuals who commented heavily on crime-oriented ones. However, this is not the case as a *Pearsonr* bivariate correlation yields a non-significant coefficient of 0.04 (p-value= 0.0952) between the two logged variables.

9.2. Comparing Drifters and Non-Drifters

To compare drifters and non-drifters, Mann-Whitney U tests are computed on the whole dataset and the top 30% for each of the indicators presented above and for the nine sub-datasets generated by combining username filters and time filters. None of the filter combinations change the substantive conclusions of this study.

Thus, for purposes of concision, the results of only one combination of username and time filters are presented: the username filter 5 chars+ and the time filter 2016-2019[27]. The former represents a conservative approach for the username filter and the latter a middle-ground for the time filter. The exact combination used, however, does not change the substance of the results. Results for all filter combinations are provided in Appendix C.

9.2.1. Considering the Platform Population

The Mann-Whitney U tests were first computed on the whole dataset to assess if drifters' behaviors differed from those of non-drifters on the informal platform. Table 8 presents the results of the series of non-parametric tests and significant relationships are highlighted in grey.

[27] This combination is chosen because: (1) the 5 chars+ filter is the most conservative, and (2) the 2016–2019-time filter is the most rigorous: comments posted one year prior and after the period of study. The first time filter is liberal (2015-2020) and the third (2017-2018) is strict, leaving out potential comments posted prior or before.

Table 8 Mann-Whitney U Test Results for the Whole Dataset with Username Filter 5 Chars+ and Time Filter 2016-2019

	Drifters N=700		Non-Drifters N= 22,648		Statistics		
	$\bar{x}\,(\sigma)$	$\tilde{x}$	$\bar{x}\,(\sigma)$	$\tilde{x}$	U	p	$1-f$
Activity Rate							
N. comments	34.27 (136.51)	5	29.11 (151.26)	4	7241098	0.000	0.54
N. days active	16.60 (38.11)	3	13.53 (40.74)	2	7143484	0.000	0.55
Diversification							
SDI	0.33 (0.40)	0	0.29 (0.39)	0	7438357	0.001	0.53
N. cat.	2.19 (1.88)	1	1.97 (1.68)	1	7373268	0.000	0.54
N. sub-cat	3.69 (6.18)	1	3.15 (5.37)	1	7441092	0.001	0.53
Business							
N. $/ ₽ sign	1.24 (5.15)	0	1.05 (10.84)	0	7373506	0.000	0.54
Prop. $/ ₽ sign	0.05 (0.15)	0	0.04 (0.13)	0	7407759	0.000	0.53
Specific Topics							
Search Engines	2.22 (13.03)	0	2.96 (21.34)	0	7886942	0.379	0.50
Monetizing sites	7.16 (33.93)	0	5.73 (41.79)	0	7756367	0.121	0.51
Practical opt.	3.06 (11.71)	0	3.84 (31.48)	0	7758960	0.121	0.51
Comm. of prof.	8.35 (62.68)	0	3.93 (40.53)	0	7229753	0.000	0.51
Site building	4.21 (19.02)	0	4.64 (45.37)	0	7557235	0.005	0.52
Exch. and sales	1.54 (6.23)	0	1.46 (9.61)	0	7454369	0.000	0.53
Purch. traffic	0.78 (6.96)	0	0.67 (9.90)	0	7733458	0.018	0.51
Work webmasters	1.04 (5.50)	0	0.96 (5.99)	0	7888565	0.367	0.50
Not about work	5.91 (54.54)	0	4.91 (71.01)	0	7658896	0.003	0.52

Mean: $\bar{x}$, std: σ, median: $\tilde{x}$, Mann-Whitney U: U, p-value: p, effect size: $1-f$, significance level α is 0.05

As displayed in Table 8, 12 out of 16 sub-indicators display significant differences (i.e., the null hypothesis is rejected in favor of the alternative hypothesis) between drifters and non-drifters. However, when comparing the descriptive statistics ($\bar{x}$ score is in bold) for each group, the absolute differences reported are minimal, as illustrated in the following text, which goes over each indicator.

In terms of rate of activity, Mann-Whitney U tests illustrate that there are significant differences in the number of comments (U= 7241098, p=0.000) for drifters ($\bar{x} = \mathbf{34.27}$, $\sigma = 136.51$, $\tilde{x} = 5$) compared to non-drifters ($\bar{x} = \mathbf{29.11}$, $\sigma = 151.26$, $\tilde{x} = 4$) as well as in the number of active days (U= 7143484, p=0.000) for drifters ($\bar{x} = \mathbf{16.60}$, $\sigma = 38.11$, $\tilde{x} = 3$) compared to non-drifters ($\bar{x} = \mathbf{13.53}$, $\sigma = 40.74$, $\tilde{x} = 2$). Thus, drifters tend to post a few more comments and are active for a few more days on average. Yet the difference is limited, as illustrated in the descriptive statistics. The effect

sizes also reveal a small difference, with only 54% of possible pairs being in favor of drifters for the number of comments and 55% for the number of days.

In terms of diversification level, there are also significant differences in the SDI (U= 7438357, p=0.000) between drifters ($\bar{x} = \mathbf{0.33}$, $\sigma = 0.40$, $\tilde{x} = 0$) and non-drifters ($\bar{x} = \mathbf{0.29}$, $\sigma = 0.39$, $\tilde{x} = 0$), as well as the number of categories (U= 7373268, p=0.000) for drifters ($\bar{x} = \mathbf{2.19}$, $\sigma = 1.88$, $\tilde{x} = 1$) and non-drifters ($\bar{x} = \mathbf{1.97}$, $\sigma = 1.68$, $\tilde{x} = 1$), and the number of subcategories (U= 7441092, p=0.000, drifters: $\bar{x} = \mathbf{3.69}$, $\sigma = 6.18$, $\tilde{x} = 1$, non-drifters: $\bar{x} = \mathbf{3.15}$, $\sigma = 5.37$, $\tilde{x} = 1$). Yet the minimal differences in the descriptive statistics of the two groups and the effect sizes of 53% and 54% illustrate that, overall, these two groups are relatively similar.

In terms of business purposes, Mann-Whitney U tests also show that there are significant differences between the number of comments posted for business purposes (U= 7373506, p=0.000) for drifters ($\bar{x} = \mathbf{1.24}$, $\sigma = 5.15$, $\tilde{x} = 0$) and non-drifters ($\bar{x} = \mathbf{1.05}$, $\sigma = 10.84$, $\tilde{x} = 0$) as well as their proportion (U= 7407759, p=0.000, drifters: $\bar{x} = \mathbf{0.05}$, $\sigma = 0.15$, $\tilde{x} = 0$, non-drifters: $\bar{x} = \mathbf{0.04}$, $\sigma = 0.13$, $\tilde{x} = 0$). However, these differences are, again, limited considering the effect sizes of 53% and 54% and the reported descriptive statistics.

Lastly, in terms of topics discussed, five categories out of nine display a significant difference between the number of comments for drifters and non-drifters: the communication of professionals category (U= 7229753, p=0.000, drifters: $\bar{x} = \mathbf{8.35}$, $\sigma = 62.68$, $\tilde{x} = 0$, non-drifters: $\bar{x} = \mathbf{3.93}$, $\sigma = 41.79$, $\tilde{x} = 0$), the site building category (U= 7557235, p=0.000, drifters: $\bar{x} = \mathbf{4.21}$, $\sigma = 19.02$, $\tilde{x} = 0$, non-drifters: $\bar{x} = \mathbf{4.64}$, $\sigma = 45.47$, $\tilde{x} = 0$), the exchange and sales category (U= 7454369, p=0.000, drifters: $\bar{x} = \mathbf{1.54}$, $\sigma = 6.23$, $\tilde{x} = 0$, non-drifters: $\bar{x} = \mathbf{1.46}$, $\sigma = 9.61$, $\tilde{x} = 0$), the purchased traffic category (U= 7733458, p=0.000, drifters: $\bar{x} = \mathbf{0.78}$, $\sigma = 6.96$, $\tilde{x} = 0$, non-drifters: $\bar{x} = \mathbf{0.67}$, $\sigma = 9.90$, $\tilde{x} = 0$) and the not about work category (U= 7658896, p=0.000, drifters: $\bar{x} = \mathbf{5.91}$, $\sigma = 54.54$, $\tilde{x} = 0$, non-drifters: $\bar{x} = \mathbf{4.91}$, $\sigma = 71.01$, $\tilde{x} = 0$). Yet the minimal differences in the descriptive statistics of the two groups and the effect sizes ranging between 51% and 53% illustrate that, although significant differences are found, these differences are minimal.

Figure 6 illustrates the distribution of each sub-indicator for each group. Through such visualization, one can see that the distributions of both groups are highly similar in

terms of shape and scale throughout all sub-indicators. Drifters tend to score higher in most indicators, but the effect sizes for all indicators are remarkably small. Considering these results, concluding that drifters and non-drifters are from a different population would stretch the reality. The analysis is recomputed with the top 30% dataset below.

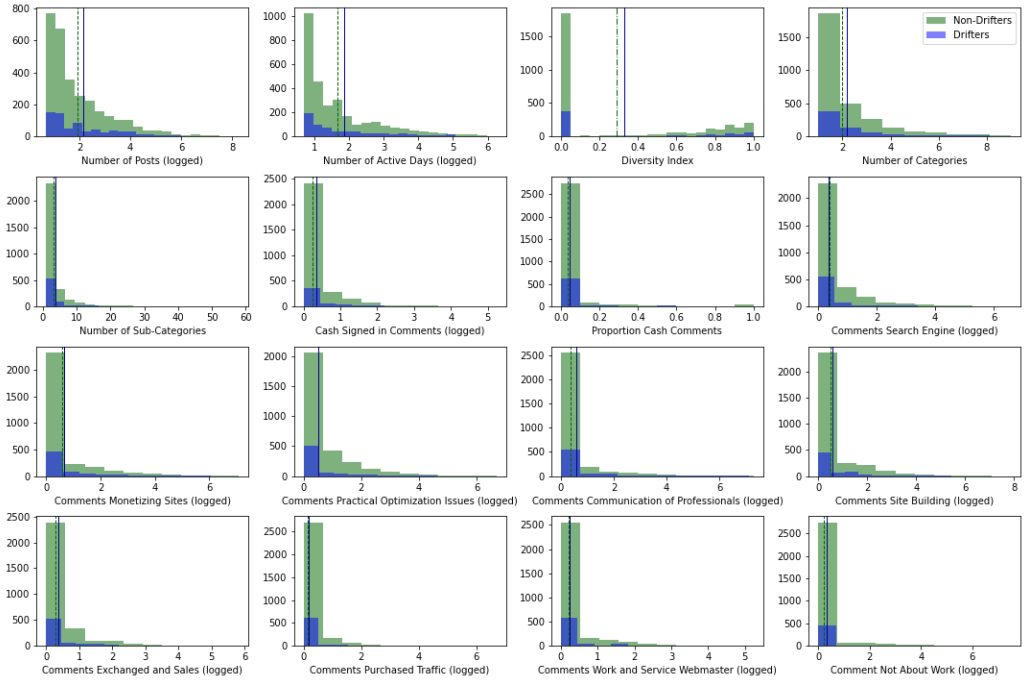

Figure 6 Distribution of Behavior Indicators for Drifters and Non-Drifters

For visibility purposes, all drifters are included in each representation while random samples of 3,000 non-drifters are selected for each indicator. The lines represent group means. If only one line is visible, the group means overlap. Some indicators are logged, as specified in the x-axis label.

9.2.2. Considering the Top 30% in 2017 and 2018

The previous analysis thus found that drifters and non-drifters have minor to no differences in their behaviors on the informal platform. One could wonder if these results are an artefact of selecting the entire population for the analysis, including all minimal contributors. When selecting only top platform contributors, the behaviors of drifters and non-drifter may differ. To evaluate this hypothesis, the analysis above was repeated with only the top 30% of individuals discussing on the informal platform. Results are presented in Table 9 and significant relationships are highlighted in grey.

Table 9 Mann-Whitney U Test Results for the Top 30% Dataset with Name Filter 5 Chars+ and Time Filter 2016-2019

	Drifters N=244		Non-Drifters N=6,680		Statistics		
	$\bar{x}\,(\sigma)$	$\tilde{x}$	$\bar{x}\,(\sigma)$	$\tilde{x}$	U	p	$1-f$
Activity Rate							
N. comments	92.68 (220)	36	91.71 (268)	27	736120	0.0051	0.53
N. days active	43.27 (55.5)	22	40.59 (67.7)	17	714399	0.0005	0.52
Diversification							
SDI	0.52 (0.35)	0.61	0.51 (0.36)	0.6	794990	0.2563	0.51
N. cat.	3.77 (2.35)	3	3.53 (2.25)	3	767956	0.0603	0.53
N. sub-cat	7.78 (9.09)	5	7.20 (8.51)	4	787480	0.1839	0.52
Business							
N. $/ ₱ sign	3.27 (8.33)	1	3.30 (19.77)	0	736008	0.0024	0.55
Prop. $/ ₱ sign	0.04 (0.10)	0.01	0.04 (0.08)	0	748942	0.0094	0.54
Specific Topics							
Search Engines	6.01 (21.58)	0	9.36 (38.52)	0	801801	0.3182	0.51
Monetizing sites	19.55 (53.7)	1	18.04 (75.5)	1	781203	0.1222	0.52
Practical opt.	8.14 (18.78)	0	11.79 (57.2)	1	807473	0.3975	0.51
Comm. of prof.	23.08 (105)	1	12.58 (73.9)	0	719287	0.0003	0.56
Site building	10.98 (31.1)	1	14.55 (82.7)	1	799605	0.2969	0.51
Exch. and sales	3.59 (10.13)	0	4.23 (17.33)	0	796505	0.2396	0.51
Purch. traffic	1.95 (11.67)	0	1.99 (17.87)	0	790470	0.1241	0.52
Work webmasters	2.54 (9.06)	0	2.71 (10.75)	0	806772	0.3674	0.51
Not about work	16.84 (91.5)	0	16.47 (130)	0	757053	0.0099	0.54

Mean: $\bar{x}$, std: σ, median: $\tilde{x}$, Mann-Whitney U: U, p-value: p, effect size: $1-f$, significance level α is 0.05

In comparison to the previous analysis, fewer significant relationships are found: six out of the 16 sub-indicators display significant differences between the two groups (i.e., the null hypothesis is rejected in favor of the alternative hypothesis). Yet, although significant, the reported differences between the two groups are, once again, minimal, as highlighted in the text below ($\bar{x}$ score is in bold).

In terms of rate of activity, Mann-Whitney U tests illustrate that there are significant differences in the number of comments (U= 736120, p=0.0051) for drifters ($\bar{x} = \mathbf{92.68}$, $\sigma = 220$, $\tilde{x} = 36$) compared to non-drifters ($\bar{x} = \mathbf{91.71}$, $\sigma = 268$, $\tilde{x} = 27$) as well as in the number of active days (U= 714399, p=0.0005) for drifters ($\bar{x} = \mathbf{43.27}$, $\sigma = 55.5$, $\tilde{x} = 22$) compared to non-drifters ($\bar{x} = \mathbf{50.59}$, $\sigma = 66.7$, $\tilde{x} = 17$). Yet, even in the top 30%, although drifters tend to post a few more comments and are active for a few more days, on average, the differences are minimal. The reported effect

sizes also illustrate this minimal difference with only 53% of possible pairs being in favor of drifters for the number of comments and 52% for the number of days.

In terms of diversification, no sub-indicators, the SDI, the number of categories, and the number of sub-categories, illustrate a significant difference between the distribution of the two groups.

In terms of business purposes, Mann-Whitney U tests illustrate that there are significant differences between the number of comments posted for business purposes (U= 736008, p=0.0024) for drifters ($\bar{x} = \mathbf{3.27}$, $\sigma = 8.33$, $\tilde{x} = 1$) and non-drifters ($\bar{x} = \mathbf{3.30}$, $\sigma = 19.77$, $\tilde{x} = 0$) and their proportions (U= 748942, p=0.0094, drifters: $\bar{x} = \mathbf{0.04}$, $\sigma = 0.10$, $\tilde{x} = 0.01$, non-drifters: $\bar{x} = \mathbf{0.04}$, $\sigma = 0.08$, $\tilde{x} = 0$). However, the differences in the descriptive statistics of the two groups are minimal. The 55% effect sizes for the number of comments and 54% for the proportion illustrate, again, that these differences are, once more, limited.

Lastly, in terms of topics discussed, two out of nine categories display a significant difference between the number of comments for drifters and non-drifters: the communication of professionals category (U= 719287, p=0.0003, drifters: $\bar{x} = \mathbf{23.08}$, $\sigma = 105$, $\tilde{x} = 1$, non-drifters: $\bar{x} = \mathbf{12.58}$, $\sigma = 73.9$, $\tilde{x} = 0$), and the not about work category (U= 757053, p=0.0099, drifters: $\bar{x} = \mathbf{16.84}$, $\sigma = 91.5$ $\tilde{x} = 0$, non-drifters: $\bar{x} = \mathbf{16.47}$, $\sigma = 130$, $\tilde{x} = 0$). One could argue that the communication as a professional category, where drifters speak twice as much as non-drifters, indicates a difference. Yet the effect size of 56% is small and this effect size does not hold when the tests are computed on other filtered datasets (see Appendix C). The effect size for the not about work category is also limited.

Figure 7 illustrates the distribution of each sub-indicator for each group, and, once again, the distributions of both groups are highly similar in terms of shape and scale throughout all sub-indicators. Again, drifters tend to score higher in most indicators, but the effect sizes are all small. Considering that pooling the top 30% of the population reduces the number of significant relationships from 12 to six, and given the effect size, I conclude that the differences between the two populations are minimal. Drifters rather seem to be similar to non-drifters, based on the indicators developed.

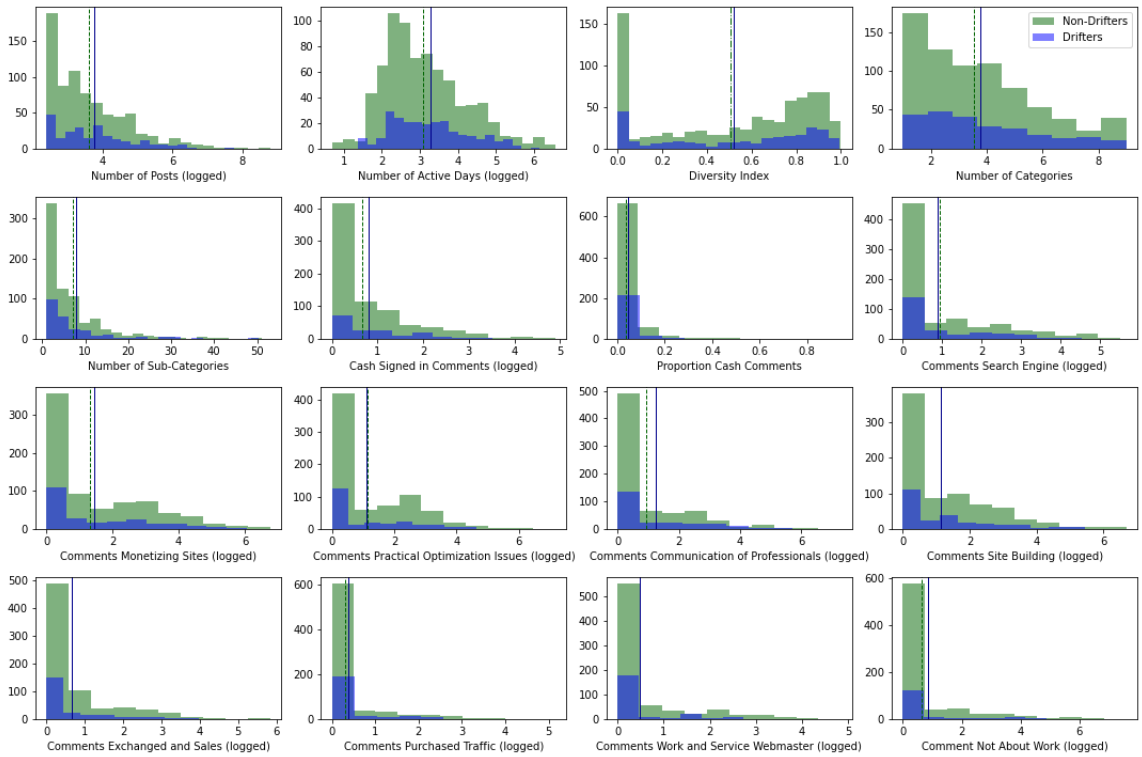

Figure 7 Distribution Drifters and Non-Drifters based on Behavior Indicators for the Top 30%

For visibility purposes, all drifters are included in each representation while random samples of 750 non-drifters are selected for each indicator. The lines represent group means. If only one line is visible, the group means overlap. Some indicators are logged, as specified in the x-axis label.

9.3. No Absolute Differences and Limited Drifting

All in all, drifters form a small proportion of the population: **7.2%**[28] when considering the most liberal filters[29]. Thus, the proportion of individuals who drift onto crime-oriented platforms, using the same username, is small. However, further considerations need to be accounted for. For example, the analysis focused on a perfect match approach, and it is likely that individuals changed their usernames (slightly or entirely) when registering on crime-oriented platforms. Also, given that the base dataset includes individuals in an informal space, it is also possible that some individuals have entirely changed their username to avoid cross-correlating their informal online identity

[28] The proportion considers only users with a username of at least five characters.

[29] Name filter: minimum of 5 characters and time filter: 2015-2010

with their identity on crime-oriented spaces. Some individuals may furthermore be involved in criminality without being registered in crime-oriented platforms, like the three individuals investigated in the private chat log. The main conclusion from this analysis is that there exists an overlap between informal and crime-oriented spaces online; through a perfect match approach and liberal filters, 7.2% of individuals seem to wade in both worlds.

The analysis also illustrated that the types of platforms on which drifters discuss are quite diversified, ranging from hacking to carding, money laundering and black hat SEO. The drifter population is diversified and distributed across a large variety of crime-oriented platforms. Although drifters may not favor one type of crime-oriented platform, the analysis showed that 61% of drifters spoke only on clearnet platforms (25% only on darknet platforms and 14% on both), illustrating that clearnet platforms may be preferred over darknet ones.

The analysis also suggested that drifters' participation in crime-oriented spaces is limited: 50% of the drifters population commented three times on these platforms and 75% made fewer than ten comments. Such participation is low considering that these statistics are pulled from the most liberal filter, which accounts for the years 2015 to 2020. In sum, the majority of drifters seem to be limited contributors in crime-oriented spaces. Potentially, these individuals limit their involvement in crime-oriented spaces because of the platforms' more obvious criminal status.

The significant relationships found with the Mann-Whitney U tests displayed minimal to no differences between drifters and non-drifters in terms of activity rate, diversification, business purposes and specialized topics on the informal platform. This finding is consistent regardless of whether the whole population or the top 30% is considered. However, there are important limits to the analyses above: other indicators, not used in this study, could differentiate both groups. Other techniques could also be used to identify drifters. Finally, although drifters are relatively indistinguishable, based on the indicators developed, their presence in crime-oriented platforms, compared to the informal one, still warrants further investigation. More precisely, that drifters' involvement in crime-oriented spaces is limited, based on a static dataset, sparks inquiries on whether such a finding is consistent over time. This inquiry led the final analysis of this thesis.

Chapter 10. **Methods to assess Drifting Trajectories**

The last analysis of this thesis aims at fulfilling the second objective of this study, which is to assess drifters' relationship between informal and crime-oriented spaces. The previous chapters illustrated that drifters are relatively indistinguishable from the mass, and their involvement in crime-oriented platforms is limited. The following analysis complements these results by looking at drifters' relationship between informal and crime-oriented spaces through time. The research question leading this analysis is: "*How do drifters use the informal space compared to crime-oriented spaces over time?*"

The strategy to answer this question was to develop a group-based trajectory model that could detect similar trajectories of drifters' posting behavior between the informal platform and crime-oriented ones through time. This chapter presents the various methodological steps taken to develop such a model. It starts by explaining the longitudinal dataset created and the Krackhardt External/Internal ratio (E/I ratio) used to capture commenting patterns. Then, the logic behind group-based trajectory modeling and the model created are outlined.

10.1. Dataset

To conduct such a longitudinal analysis, a dataset of the informal workforce spanning several years was needed. To create this dataset, the Flare API was leveraged, and all comments posted on the informal platform from 2012 to 2020 were first extracted[30]. Each comment's identification number, text, and timestamp, as well as the name of the actor who wrote it, was gathered[31]. With this, a list of usernames containing all individuals who posted on the informal platform over the nine-year period of study was created.

Before searching these usernames on the Flare Systems database to find other platforms on which they discussed, a username filter was applied: the most conservative

[30] Nine years may seem like a long timeframe for online participation. However, the three individuals in the private chat log had been active on this platform since even longer than that (as early as 2009) and two of them were still active at the time of writing this thesis. Also, 2012 was selected as the starting point since data on the informal platform prior to this year was unreliable. The year 2020 was selected as the last full year because the data was extracted in mid-2021.

[31] The actor named: "Этот пользователь удален" (meaning: this user has been deleted) was removed.

one (presented in the previous chapter). This filter removes all usernames that do not have a minimum of 5 characters AND at least an uppercase OR a number OR one special character. This allowed minimizing the potential false positive of linking unrelated usernames during the cross-correlation procedure between platforms. Overall, the list of usernames from 2012 to 2020 included 35,450 individuals. Each of them was searched in the Flare Systems database and, when a comment on another platform was found under the same username, the comment's identification number, timestamp, the platform name, and the username were extracted.

Of these 35,450 individuals, 2,471 perfect matches were found: they represent 2,471 individuals who have discussed at least once on another platform with the same username during the nine-year period. These 2,471 individuals discussed on 34 different platforms, the same crime-oriented platforms presented in the previous chapter, except for one. The new one was investigated and was not found to be crime-oriented; it was thus removed from the dataset.

Overall, these 2,471 individuals posted 285,372 comments on the informal platform and 79,448 on crime-oriented platforms over nine years. Drifters' posting trends through time, on both informal and criminal spaces, are presented in the results section below.

10.2. Krackhardt External/Internal Ratio

To assess posting patterns of drifters in and out of the informal platform to and from crime-oriented spaces, the Krackhardt External/Internal Ratio (E/I ratio) was used. This ratio was developed in network science (Krackhardt and Stern, 1988) to measure the extent to which an individual's relationships are centered around their internal community or around other, external communities. A score of -1 indicates that an individual only has ties to their assigned community while a score of 1 indicates that an individual only has ties external to their assigned community. A score of 0, on the other hand, means that the individual has equal ties in and out of their community.

In this study, the E/I ratio refers to drifters' commenting pattern on the informal platform vs crime-oriented ones. Internal ties are comments posted on the informal

platform while external ties are comments posted on crime-oriented platforms. The ratio is defined in eq. (4):

$$E/I\ Ratio\ _t = \frac{x_{e,t} - x_{i,t}}{x_{e,t} + x_{i,t}} \quad \text{eq. (4)}$$

where $x_{e,t}$ represents the number of external comments (outside the informal platform) at period t, and $x_{i,t}$ represents the number of internal comments (inside the informal platform) at period t. This E/I ratio is calculated for every user and every period between 2012 and 2020. The results range from -1 to 1, where -1 represents all comments on the informal platform and 1 represents all comments external to the informal platform. If a user posted equally on both spaces, then the E/I ratio is zero, as neither space is favored. Descriptive statistics on the E/I ratio for each period of study are presented in Table 10.

Table 10 Distribution of E/I Ratio across the Different Periods of Study

Period	N	Mean (std)	Med
2012	1,124	-0.89 (0.42)	-1
2013	1,179	-0.73 (0.63)	-1
2014	1,146	-0.54 (0.81)	-1
2015	1,243	-0.23 (0.92)	-1
2016	1,133	-0.30 (0.91)	-1
2017	1,076	-0.22 (0.92)	-1
2018	1,034	-0.07 (0.96)	-0.63
2019	975	0.11 (0.95)	0.93
2020	922	0.34 (0.90)	1

As shown in Table 10, the average E/I ratio and the median are closer to -1 (favoring informal platform) at the beginning of the period of study and move closer to 1 (favoring crime-oriented platforms) at the end of the period of study. Notice also that the standard deviations for every year are large (considering that the ratio has a range between minus one and one), which means that there is great variance in the E/I ratio score in the drifter population through time.

10.3. Identifying Drifters' Trajectories

To assess drifters' posting behavior through time, a group-based trajectory model (GBTM) was developed. GBTM are finite mixture models designed to extract subgroups within a population that follow similar trajectories over a variable of interest (Jones and Nagin, 2007). Finite mixture refers to models that analyze outcomes from a population with a finite number of homogenous subpopulations (Nagin and Odgers, 2010a,b). Such models are widely used in criminology to assess developmental trajectories of delinquency (Nagin and Piquero, 2014; Haviland and Nagin, 2005; Nagin and Odgers, 2010a,b; Nagin and Tremblay, 2005). The base model is presented below.

10.3.1. The Base Model

GBTM aims at finding clusters of individuals with similar trajectories, yet the model's parameters are not the result of a cluster analysis. Rather, the model is the product of a maximum likelihood estimation: the objective is to identify a set of parameters that will maximize the probability of an outcome (Nagin, 2005, p.24). As well summarized in Jones and Nagin (2007, p.543) and paraphrased below, GBTM assumes that, given a longitudinal measured sequence $Y_i = y_{i1}, y_{i2}, y_{i3}, \dots, y_{1T}$ of an individual i over T periods, and $P(Y_i)$ representing the probability of observing the sequence Y_i, the population is formed of a mixture of J distinct trajectory groups as defined in eq. (5).

$$P(Y_i) = \sum_j \pi_j P^j(Y_i) \quad \text{eq. (5)}$$

where $P^j(Y_i)$ represents the probability of observing Y_i given group membership j, and π_j represents the probability of group j in the population (i.e., the probability of an individual picked randomly of being from group j). The base model assumes that, conditional on membership j, the variables $Y_{it}, t = 1,2, \dots T$ at each period are independent and thus the probability of observing $Y_{i,}$ given group membership j ($P^j(Y_i)$), can be defined in eq. (6).

$$P^j(Y_i) = \prod_T p^j(y_{it}) \quad \text{eq. (6)}$$

where $P^j(Y_{it})$ is the probability distribution function of Y_{it}, given membership in group j (Nagin, 2005, p.26). On the other hand, the group membership probabilities $\pi_j, \ j = 1, \dots J$

are estimated via the multinomial logit function (p.543) to ensure that the probability stays bound between 0 and 1, as defined in eq. (7).

$$\pi_j = \frac{e^{\theta_j}}{\sum_1^J e^{\theta_j}} \text{ eq. (7)}$$

where θ_1 is normalized to zero. The form of $p^{jt}(y_{it})$ (data points) depends on the type of data investigated. Common distributions for these models include zero-inflated Poisson, logit or censored normal (Jones and Nagin, 2007, p.543). The shapes of the trajectories for each group are defined via a polynomial function over time and can vary across groups. Finding the form and parameters of these polynomials, along with the number of groups, is the bulk of the modelling process.

10.3.2. Censored Normal Model

The model's variable of interest is the E/I ratio, computed for each drifter at each period. As mentioned above, the specific form of likelihood function depends on the distribution of the outcome variable (e.g., censored normal, Poisson or logit). Given that, in this study, the outcome variable is bound between -1 and 1 and clusters at these extremes, the censored normal likelihood function is selected. Such a function allows for censoring when the outcome variable clusters at a minimum and/or a maximum scale (Jones et al., 2001) as the linkage between the time and the outcome variable is determined with a latent variable (${y^*}^j{}_{it}$).

The relationship between time and the latent variable can go up to a fourth-order polynomial (ex: ${y^*}^j{}_{it} = {\beta_0}^j + {\beta_1}^j T_{it} + {\beta_2}^j {T^2}_{it} + {\beta_3}^j {T^3}_{it} + {\beta_4}^j {T^4}_{it} + \varepsilon_{it}$) and the error term is normally distributed with a mean of zero and a constant standard of deviation (Nagin, 2005; Jones and Nagin, 2007). The latent variable estimates the potential for an individual to engage in behavior beyond the bound outcome when estimating the model's parameters (Nagin, 2005). Such a function is ideal when an outcome variable is bound, such as a psychometric scale, and a large number of observations cluster at a minimum, while another smaller contingent clusters at the maximum (Nagin, 1999). In the model, those clustering at one extreme of the E/I ratio (e.g., -1) have differences that cannot be grasped by the bound variable. For example, there might be differences

among those who scored -1, such as individuals who had a higher level of engagement in crime-oriented platforms. The latent variable captures these potential differences.

10.3.3. Drifters Sample for the Model

The outcome variable is the E/I ratio for each drifter during the nine years studied, from 2012 to 2020. However, of the 2,471 drifters found, not all were active throughout the nine years of study. Table 11 illustrates how many individuals were active from one year to nine years.

Table 11 Distribution of the Number of Years Available per Drifter in the Dataset

Number of Year	Drifters	% Sample	Cumulative
1 year	84	4%	3%
2 years	667	27%	31%
3 years	520	21%	52%
4 years	381	15%	67%
5 years	266	11%	78%
6 years	193	8%	86%
7 years	147	6%	92%
8 years	104	4%	96%
9 years	109	4%	100%
N	2,471	100%	

As shown in Table 11, only 4% of the sample were active for the nine years studied (109 individuals) and 67% of the sample includes individuals active for fewer than four years. This means that only 33% were active at least five years. That most drifters are not active for the nine years is unsurprising, given that online commitments, especially in crime-oriented spaces, are known to be ephemeral (Goldsmith and Brewer, 2015).

Thus, the greater the sample of drifters the more likely the individuals included will have missing information. To keep the entire sample, the missing data could be treated in two ways. First, for every year a drifter was not active, the model could consider that the drifter has an E/I ratio of zero. In such a case, a score of zero would mean that either the drifter has posted equally in both the informal platform and other crime-oriented platforms OR the drifter has not posted in any platform. In both cases, the

drifter would not be favoring the informal platform over other crime-oriented ones. This approach also considers that what Flare Systems has gathered is the ground-truth: if there are no comments from these drifters in the monitored platforms during these years, it means these individuals have not posted and their E/I ratio score should be zero.

The second approach is inferential: it considers that, for every year a drifter did not post, the E/I ratio is missing. Missing data will be treated at random by the software. This approach considers that Flare Systems does not have the ground-truth, the dataset has missing at random (MAR) information, and users' behaviors were not captured for many potential explanations, such as technical difficulties or because drifters have changed their usernames through time. The extent to which the missing data is related to a random process is, however, unclear.

After thorough evaluation, both approaches are somewhat problematic considering the significant amount of missing information in the dataset. The first approach imposes a high number of zeros, which leads to the trajectories being dragged near the zero line for the outcome variable when running the model. The second approach (treating the data as MAR) inputs a substantial amount of "random" information to the model, which can potentially lead to misleading results.

In the end, **the fewer missing periods the better**. The idea was to find relationships, such as what proportion of drifters stay mainly in the informal platform, move permanently into crime-oriented platforms or discuss in both alternatively. The model was thus computed on a subset of drifters: those for whom there were observations for the nine periods of study (N=109). Using these active drifters allowed me to explore trends, without imposing artificial data. Once the best model parameters and number of groups were determined with this subset, the model was applied to additional subsets of drifters using the conservative model explained above (adding zeros to missing information). The STATA software (Version 16) and the TRAJPLOT plugin (Jone and Nagin, 2013) were used for model computations.

10.3.4. Best Model Decision

Given that the model aims at dividing a population into groups with similar trajectories, there are vast possibilities as each individual can represent a group and the

trajectories can go from a constant or linear form to a quadratic or a cubic one. To determine the best model, Nagin (2005) developed a formal procedure based on the Bayesian Information Criterion (BIC). BIC is one of the most used model fit criteria that balances model complexity (number of parameters) and goodness of fit (Nagin and Odgers, 2007). It is defined eq. (8),

$$BIC = log(L) - 0.5klog(N) \text{ eq. (8)}$$

where L is the value of the model's maximized likelihood, N is the sample size, and k is the number of parameters (Nagin, 2005). The left hand side of the formula ($log(L)$) accounts for an improvement in the model fit while the right side ($0.5klog(N)$) subtracts a penalty for the addition of a group or a parameter to the model fit. Models with a higher BIC are thus preferred. Moreover, the model includes two BICs: one that considers the number of participants as the sample size and another that considers the number of observations as the sample size. The correct theoretical BIC is between these two BICs (Nagin, 2005).

Nagin's (2005) procedure to find the best model is based on two processes: (1) determining the number of groups that best divide the population and (2) determining the best polynomial function to use for each trajectory. For the first process, a predetermined polynomial function is chosen, based on prior knowledge of the data, and groups are added iteratively to the model.

However, sometimes, adding groups results in a slight increase in BIC. To determine if such a slight increase is significant, the Bayes factor B_{ij} can be used. This factor computes the ratio of probability of i being the right model to the probability of j being the correct model (Nagin, 2005, p.6). However, given that calculating the Bayes factor can be computationally intensive, Nagin (2005) argues that the Kass and Wasserman (1995) approximation of the Bayes factor is sufficient. The approximation is expressed as: $B_{ij} = e^{BIC_i - BIC_j}$.

When comparing two models, if B_{ij} is larger than 10 ($B_{ij} > 10$), then there is strong evidence in favor of the i^{th} model, the model with an additional group. A B_{ij} between three and 10 ($3 < B_{ij} < 10$) means that there is moderate evidence, and a smaller B_{ij} between one and three ($1 B_{ij} < 3$) means that there is weak evidence in

favor of the i^{th} model. On the other hand, a B_{ij} between one and one third ($1/3 < B_{ij}$ 1) illustrates weak evidence for the j^{th} model, between one third and one tenth ($1/10 < B_{ij} < 1/3$) shows moderate evidence, and lower than one tenth ($B_{ij} < 1/10$) means that there is strong evidence for the j^{th} model. When $B_{ij} = 1$, both models are equally good.

In specific situations, the BIC constantly increases when adding a group or a parameter, preventing one from determining the best model. In such a case, Nagin (2005) argues that the model selection must balance parsimony and the distinctive features of the data. Models with a fewer number of groups are favored: it is better to select no more groups than are necessary to illustrate the unique features of the data (Nagin, 2005).

Hence, the number of groups that best fit the data can be found with the BIC following the procedure mentioned above. Once the best number of groups is determined, the model's parameters are determined for each trajectory group using the BIC as an indicator. Entropy can also be an indicator of a model's fit. The measure indexes "classification accuracy by averaging the posterior probabilities after individuals have been assigned to their most likely class, with values closer to 1 indexing greater precision (range 0 to 1)". (Nagin and Odgers, 2010, p.117).

10.3.5. Model Diagnostics

Based on Nagin (2005), three indicators can be used to assess the model's fit to the data. The first indicator is the group average of individual posterior group membership probabilities ($AvePP$). Posterior group membership probabilities are calculated for each individual and the $AvePP_j$ is the average of these probabilities for each group j in which an individual was assigned to the model. An $AvePP$ of 70% is assumed to be adequate (Nagin, 2005). The second indicator is the odds of correct classifications (OCC), which is calculated in eq (9):

$$OCC_j = \frac{\frac{AvePP_j}{1-AvePP_j}}{\frac{\pi_j}{1-\pi_j}} \quad \text{eq. (9)}$$

where $AvePP_j$ is the average posterior probability of group j and π_j is the random assignment of probabilities for the said group j. An OCC of one means that the model has no predictive probability beyond random chance while an OCC>5 means that the model is a good fit. The third indicator P_j calculates the number of individuals assigned to a group. It is defined in eq. (10)

$$P_j = N_j/N \text{ eq. (10)}$$

where N_j is the number of individuals assigned to group j and N is the total number of individuals. P_j is then compared with π_j which represents the model's estimated random assignments to group j. When $AvePP_i$ = 1, all individuals are assigned to one group with perfect certainty and $\pi_i = P_i$. As the assignment error increases, the difference between the two measures increases. A correspondence between the two measures is thus an indicator of model accuracy (Nagin, 2005). The three model diagnostics are calculated and reported below.

Chapter 11. **Drifter Trajectories Favor Informality**

This final analysis chapter presents the result on the group-based trajectory modeling developed to answer the question: "*How do drifters use the informal space compared to crime-oriented spaces over time?*" Results show that about 75% of drifters favor the informal space over crime-oriented ones over time! The chapter starts by presenting longitudinal information about the dataset. The model's results are then introduced and discussed.

11.1. Drifters' Commenting Behavior Through Time

To begin, longitudinal commenting trends are presented for the informal platform population (N=35,450) and the drifter population (N=2,471). As illustrated in Figure 8 (left), there is a clear decreasing trend in the number of comments posted on the informal platform annually, suggesting that engagement on this platform may be falling. Such a decreasing trend is also observed among the drifter population, as shown in Figure 8 (right). On the other hand, drifters' total number of comments in crime-oriented platforms does not follow a steep decrease, but rather oscillates around 10,000 comments total over time. Consequently, based on the total number of comments posted on crime-oriented platforms, drifters' engagement seems to be quite steady.

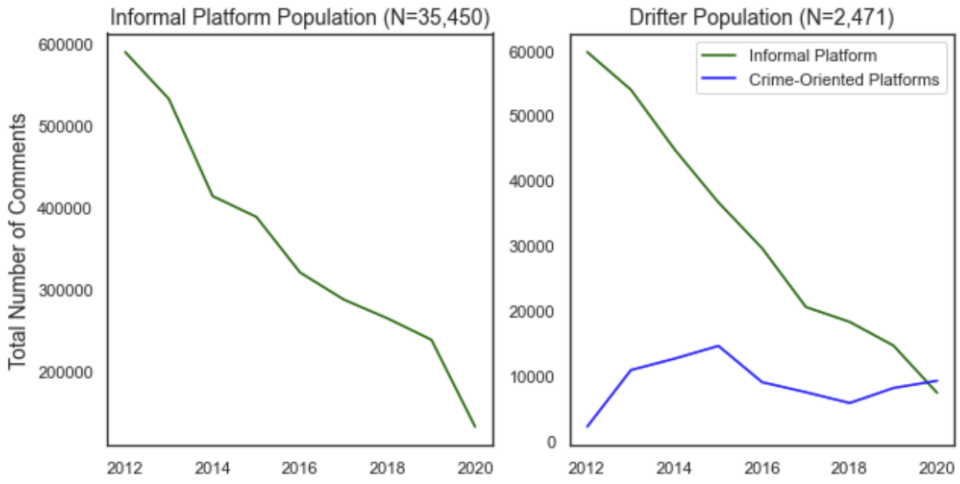

Figure 8 Total Number of Comments Annually

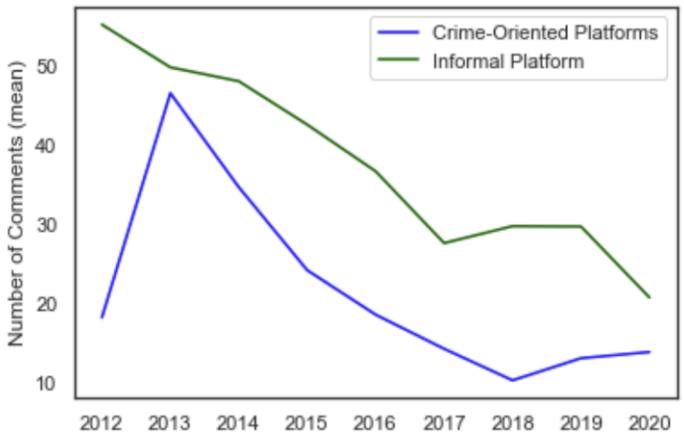

Figure 9 Mean Number of Comments for the Drifter Population through time (N=2,471)

However, a different picture is painted when considering the mean number of comments for the drifter population through time, as shown in Figure 9. The figure illustrates that drifters' engagement in terms of mean number of comments per drifter per year also decreases in the informal platform over time. In terms of commenting on crime-oriented platforms, the trend increases from 2012 and 2013 and then decreases constantly through time, until the end of 2018, when participation has slightly increased. Overall, drifters' average participation is declining in both spaces.

Drifters' mean number of comments decreases over time, but the number of comments on crime-oriented platforms is relatively constant, as shown in Figure 8. This means that the number of drifters who speak on crime-oriented platforms increases by the end of the period of study.

11.2. Group-Based Trajectory Modeling Results

To assess drifters' intertwined relationship between informality and criminality, a trajectory analysis on drifters' yearly E/I ratio score was computed using the censored normal distribution, as explained above. The sample considered is that including drifters active on either space throughout the whole period of study (N=109). Finding the best model required two steps: (1) determine the number of groups (i.e., number of groups in the population with similar trajectories) and (2) determine the shape of the parameters. For the first step, linear trajectories were used to evaluate the model with the best

number of groups. Such trajectories assume that drifters' E/I ratios are linear through time, either decreasing or increasing.

Table 12 illustrates the results for the first step, finding the number of groups, and includes the models' BICs. When a group is added, the B_{ij} is computed between the two models to assess whether adding a group significantly increases (decreases in this case since the values are negative) the BICs.

Table 12 Determining the Optimal Number of Groups

	BIC_1 N=981	$B_{1_{ij}}$	BIC_2 N = 109	$B_{2_{ij}}$
2 groups	-778.27	-	-771.67	-
3 groups	**-763.24**	**3,368,573**	**-753.35**	**9,042,216**
4 groups	-765.65	0.08981	-752.47	2.4108997
5 groups	-774.41	0.000	-757.93	0.00425
6 groups	-778.48	0.017	-758.71	0.458406

Table 12 illustrates that there is strong evidence for a model with three groups ($B_{ij} > 10$) over the two-groups model. There is also strong evidence for the three-groups over the four-groups model ($B_{ij} < 1/10$). Adding more groups then does not yield higher BICs. The best model is thus the three-group model. The second step is to determine the shape of the trajectories. Table 13 presents the results for combinations for linear and quadratic trajectories. Both cubic and constant trajectories were considered, but they are not reported because they only yielded lower BICs than the BICs presented in Table 13.

Table 13 Determining the Shapes of the Trajectories

	Group 1 β_1	Group 2 β_1	Group 3 β_1	BIC_1 N=981	BIC_2 N = 109
1	Linear	Linear	Linear	-763.24	-752.35
2	Quadratic	Linear	Linear	-766.68	-755.69
3	Linear	Quadratic	Linear	-759.20	-748.22
4	Linear	Linear	Quadratic	-759.20	-748.22
5	Linear	Quadratic	Quadratic	-761.76	-749.68
6	Quadratic	Quadratic	Linear	-762.64	-750.56
7	Quadratic	Quadratic	Quadratic	-765.19	-752.01

As illustrated in Table 13, the models with the highest BICs were models 3 and 4, which both included two linear and one quadratic trajectory shape. Both models were compared, and the results were exactly the same (which is not always the case); results for (the simpler) Model 3 are thus presented below.

11.2.1. Three-Group Model Results

Table 14 presents the results of the three-group model with two linear and one quadratic trajectory. The trajectories through time are also presented in Figure 14.

Table 14 Trajectory Results with E/I ratio as the Outcome Variable

	Estimate	**SE**	**P-value**
Group 1			
Intercept	-3.05046	0.22267	0.0000
Linear	0.16457	0.03248	0.0000
Group 2			
Intercept	-2.47120	0.26930	0.0000
Linear	1.40106	0.26930	0.0000
Quadratic	-0.10258	0.02658	0.0001
Group 3			
Intercept	-4.44736	0.50486	0.0000
Linear	0.64794	0.08299	0.0000
Sigma	1.31638	0.07860	0.0000
Random Assignment Prob		**SE**	**p-value**
Group 1	73%	4.91262	0.0000
Group 2	12%	3.12749	0.0002
Group 3	15%	4.20429	0.0004
BIC			
N=981	-759.20		
N=109	-748.22		
Entropy	0.924		

The results show that all trajectories found by the model are statistically significant[32]. All group intercepts are below -1 (captured by the latent variable),

[32] Sigma represents the estimated standard deviation of the residual (Zhang and Max, 2019)

suggesting a strong preference for the informal forum for all drifters at the beginning of the study. Based on the model's estimates and the trajectories presented in Figure 10, Group 1 includes 73% of the sampled drifter population and shows a positive linear -yet quite flat- trend through time. Group 2, on the other hand, represents 12% of the sampled population and illustrates a positive trend that eventually flattens and tends to decrease at the end of the period studied. Group 3 also represents a small portion of the sampled population, 15%, and illustrates a positive trend through time.

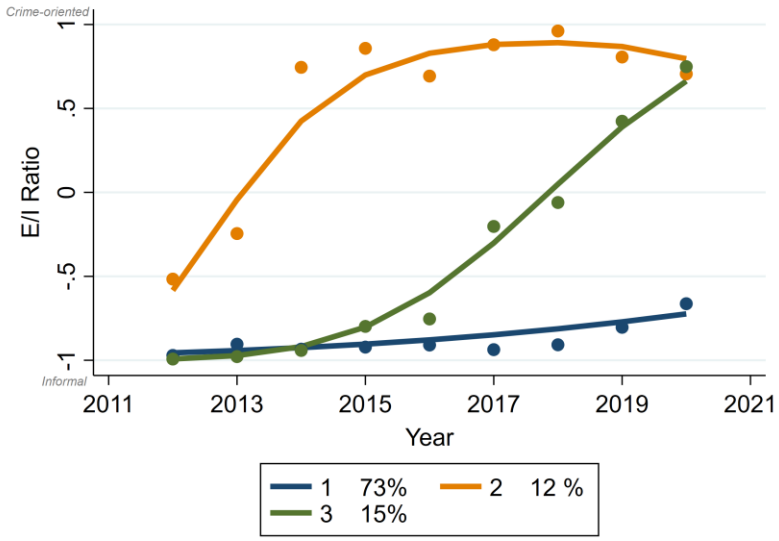

Figure 10 Group Trajectories Through Time (N=109)

The visual representation of these trajectories in Figure 11 illustrates that Group 1's trajectory, which encompasses the great majority of sampled drifters, stays close to - 1 and favors the informal platform over crime-oriented ones. Group 2, on the other hand, drifts, at the beginning of the period of study, out of the informal space to crime-oriented spaces, where the group's participants discuss through the rest of the period of study. The third group drifts out as well, but at a slower pace and a little bit later in the period of study. The members of this group start favoring crime-oriented spaces around 2017 when the zero boundary of favoring neither is crossed towards crime-oriented ones.

However, note that this model was computed on a small number of drifters: those who were active for the nine periods of study (N=109). To assess if the findings were an artifact of this sample, the current model (three groups with two linear trajectories and

one quadratic) was computed with additional subsamples: drifters with eight years of observations, seven, six, etc. The results were similar (in terms of trajectory trends and population distribution across the three groups), but as more and more data was missing, the trajectories were dragged closer to zero. Thus, the model presented above is the soundest one, the one with no missing data. It represents trends that can be seen using other datasets with missing years, until the missing year information drags the analysis to zero. Before discussion of the results, the model's diagnostics are presented below.

11.2.2. Three-Group Model Diagnostics

As presented in the methodology, Nagin (2005) has developed diagnostics to assess the extent to which a model fits the data. The diagnostics for the model presented above are available in Table 15.

Table 15 Model's Diagnostics

	N	$AvePP_j$	$\frac{STD}{AvePP_j}$	π_j	P_j	OCC_j
Group 1	81	0.97	0.08	0.73	0.74	11.96
Group 2	13	0.99	0.03	0.12	0.12	726
Group 3	15	0.92	0.12	0.15	0.14	65.16

The results illustrate that the three-group model fits the data well. The $AvePP_j$, the average of individual posterior group membership probabilities, is 97% for Group 1, 99% for Group 2, and 92% for Group 3. The respective standard deviations are also low, illustrating little deviation from the average score. The odds of correct classification (OCC) are all above Nagin's baseline of five and the three P_j (the number of individuals assigned to each group divided by the whole population) are nearly equal with the π_j, the random assignment of probabilities. Overall, the model fits the data properly.

11.3. Favoring Informality

There are key takeaways from the results of this chapter. To begin with, engagement, in terms of total number of comments, in the informal space decreases through time. This shows that the informal forum may not be as popular as it was at the

beginning of the study. Such a decreased activity rate may be due to the adverse business environment in which these individuals seem to operate (as seen in the private chat log), but this is a discussion for the following chapter.

Considering the drifter sample, the total number of comments posted on the informal platform decreases while the total number of comments posted on crime-oriented spaces is relatively steady. On the other hand, drifters' individual engagement decreases, on average, in crime-oriented platforms. This means that the number of drifters in the dataset who speak on crime-oriented platforms *increases* by the end of the period of study. Why the number of drifters speaking on crime-oriented platforms increases over time is a question that warrants further research. Potentially, crime-oriented platforms attract more users nowadays. Although interesting, this is beyond the scope of this study.

The main finding of this chapter relates to the GBTM model. When the most active drifters are selected, those who participated in the nine periods of study, the results of the trajectory analysis illustrate that drifters strongly favor informal spaces over criminal ones through time. Indeed, for 73% of the population, participation in criminal spaces is minimal compared to participation in informal spaces. On the other hand, 27% of the drifter population do end up speaking more in crime-oriented spaces over time: 12% at a quick pace and 15% at a slower pace.

The two previous analyses aimed at fulfilling the second objective: to assess drifters' relationship between informal and crime-oriented spaces. The first one illustrated that drifters are relatively indistinguishable from the mass and their involvement in crime-oriented platforms is limited. The second one illustrated that, through time, based on their commenting behavior, drifters' favor the informal platform over crime-oriented ones over time. The implications of these findings are discussed below.

Chapter 12. **Discussion**

Through two objectives and four analyses, this study uncovers contexts, perceived motivations, and organizations of individuals involved in online economic crime while putting a magnifying glass on an informal workforce and its likelihood to drift. From the results, four discussion points emerged: 1) understanding the underlying forces that influence individuals to participate in online economic crime, 2) exploring their organizations and the role of informal workers involved, 3) illustrating the benefits and difficulties of hiring such a workforce through digital labor platforms, and 4) presenting the workforce's limited involvement in crime-oriented platforms. Each is discussed below, followed by study limits and further research.

12.1. Understanding the Forces Underlying Online Economic Crime

The first discussion point focuses on understanding the underlying forces that influence individuals to participate in online economic crime. It relates to the first analysis that investigated the contextual factors and perceived motivations of those behind online economic crime from the perspectives of individuals with knowledge and experience on the matter, that is, of experts. The results spanned expertise and geographical regions, illustrating that there are global trends behind online economic crime. Each finding is discussed below and interpreted through previous criminological studies. When possible, they are also paired with the themes that emerged from the private chat log analysis.

12.1.1. The Triad Influencing Those Behind Online Economic Crime

The first factor, ***lack of legal economic opportunities****,* refers to situations where individuals do not have interesting legal opportunities to exploit their skills, leading them to participate in such profit-driven crime. Linking the lack of legal economic opportunities to crime participation implies that a relationship exists between being unable to fulfill economic goals and turning to crime to do so. In other words, individuals who seek financial wealth, and cannot achieve such gains legally, may resort to illegal means. Such an idea recalls Merton's seminal work (1968; 1938) on *Social Structure and Anomie*, which presents anomie and strain theories.

Anomie theory refers to an imbalance between cultural goals that are acclaimed, such as making money, over proper institutional means available to achieve them. When summarizing Merton's contributions, Featherstone and Deflem (2003) explain that a society is in a state of anomie when *greater stress* is put on achieving the goals and less on the approved norms regulating the means to achieve them. Strain theory, on the other hand, states that individuals are more likely to pursue illegitimate means to attain acclaimed cultural goals when *they cannot do so through legitimate means*. To explain how individuals adapt to patterns of *goals and means*, Merton (1938) sketched five modes of adaptation: conformity, ritualism, rebellion, retreatism[33] and innovation. The last one, innovation adaptation, relates to the factor found in this thesis. *Innovation* adaptation represents individuals who embrace cultural goals but are blocked from legitimate avenues to attain such goals. As stated by Merton, this blockage leads them to reject the legitimate means (as opposed to the goal) and find new avenues, *innovate*, to achieve their goals.

The factor "a lack of legal opportunity" links to Merton's idea that a differential access to legal opportunities may lead individuals to "innovate" and find other means to achieve their goals. For online economic crime, the goal appears to be profit-driven. Remember Expert 900 mentioned: "*they want to be rich cybercriminals*" (Expert, 900) and an individual in the private chat log said: *"I realized that I was led by the fact that others make good money […]*" (Developer 1, January 2018). This should not come as a surprise: gaining economic wealth is a widespread cultural goal across cultures (Passas, 2000). The factor that emerged from the data analysis implies that, in a context where there is a lack of legal opportunities to achieve economic goals, individuals may turn to crime opportunities and, in such a situation, crime becomes a means to pursue an end – make money.

Focusing on the "void" in legal opportunities implies that, given better economic conditions, at least some individuals might not participate in online economic crime. As implied in Merton's (1968; 1938) work, crime participation is a product of society's

[33] In short, c*onformity* adaptation represents the great majority of individuals in society: those who accept the cultural goals and the institutional means to achieve them. *Ritualism* adaptation represents those who reject cultural goals but will accept the institutional means. *Retreatism* are those who reject both, living as marginalists in the society. *Rebellion* includes individuals who emancipate from the cultural goals and institutional means and attempt to introduce a new social order (Merton, 1938).

forcing individuals to do things they would not do otherwise (Bernard, 1984). This line of thinking opens research avenues toward understanding what concentration of legal economic opportunities (or say growth in the technological sector) can deter most individuals from participating in online economic crime.

Merton's anomie and strain theories are intertwined, yet separate (Featherstone and Deflem, 2003) and they have been extended (Agnew, 2017; Messner and Rosenfeld, 2012; Messner, 1988, among many others), acclaimed (Adler, 2020; Rosenfeld, 1989) and criticized (Besnard 1990; Kornhauser 1978) in the criminological scholarship. Reviewing these works is beyond the scope of this thesis. Future studies could look at how anomie and strain theory can explain the high prevalence of individuals involved in online economic crime in specific contexts.

When investigating actors involved in online economic crime, the theme of *adverse business environment* emerged with *unreliable business partners, unstable payment programs* and *declining business prospects* as subthemes. The individuals studied in the private chat log were involved in internet marketing, participating in affiliate marketing programs to monetize Android portals they had developed. They talked at length about how bad the business had become, with few interesting prospects to monetize their websites. Such discussions are closely linked to the lack of legal economic opportunities raised by experts, which could partly explain why these individuals ended up seizing the Geost opportunity. This opportunity may have looked enticing in terms of its potential profitability, with few alternative options. Yet, whether the individuals studied would have preferred an equivalent **legal alternative** is unclear, given their leniency towards criminality as illustrated across their discussions. Moreover, considering that the individuals in the private chat log had invested a lot of time and energy in building their Android portals, switching to alternative opportunities, such as the movie websites they mentioned, seemed to involve high switching costs (costs related to converting to alternative business opportunities).

This case study nuances the factor that emerged from the interviews: considering these individuals may have invested time and energy in developing Android portals, the lack of legal opportunities related to their business may have enticed them to consider opportunities from the criminal realm although other legal opportunities were available, such as monetizing other types of websites. In short, legal alternatives may exist but

may not be considered due to high switching costs. Further research could investigate the different dynamics at play across subsectors, such as to what extent legal alternatives are considered by IT workers who have the potential to participate in online economic crime.

The second factor*, **lack of deterrents***, encompasses elements that lead to a feeling of *impunity* for individuals committing criminal activities. Impunity means being exempted from punishment for actions that usually are considered to deserve punishment. The lack of deterrents that induce a feeling of impunity recalls Stafford and Warr's (1993) argument that **avoiding punishment** increases the chances of committing more crime in the future. The authors revisited deterrence theory (Becarria, 1963 [1764]) by proposing that an individual may be deterred or encouraged not to offend or to offend through a combination of personal and vicarious experiences of being punished AND avoiding punishment. They posited that the latter may do more to encourage criminal behavior due to the actor's feeling "immune" to consequences (p.125). This proposition was supported in various empirical studies that found that avoiding punishment increases the chances of future offending (Sitren and Applegate 2012, 2007; Piquero and Pogarsky, 2002; Piquero and Paternoster, 1998; Paternoster and Piquero, 1995). A feeling of impunity is also the main factor explaining why, in certain settings, criminal organizations tend to be large (Tremblay, Bouchard and Petit, 2009). Studying how this feeling unfolds specifically for those involved in online economic crime, given that wealth distribution happens through online means, could be of interest to future studies.

Similarly to findings from the interviews, the individuals involved in online economic crime, studied in Chapters 6 and 7, did not seem to fear any consequences from their actions. The theme of *leniency towards criminality* illustrated that they were aware that what they were doing was illegal, yet they never mentioned facing potential consequences related to their economic activities. However, note that none of these individuals developed the malicious Geost applications nor connected to victims' bank accounts with compromised credentials. All they did was publish malicious Android applications on their website. They were paid when someone visited the website and downloaded the said application. This action resembles any other economic activities that these individuals might have pursued for a legitimate affiliate marketing program. That the actions they did were the exact same ones as the ones they did for legal

affiliate marketing programs could have created such a **sense of impunity.** However, one difference was that their websites were continually blocked by search engines, requiring them to develop various strategies to circumvent the search engines. This extra work seemed to be acceptable given the potential profitability of Geost and the few other legal alternatives in their business niche.

Mechanisms that led to this feeling of impunity mentioned by experts included *law enforcement efficiency, lack of peer judgements* and *the possibility of corrupting law enforcement*. These elements have also been identified as major factors influencing the size and scope of criminal organizations in the literature (Morselli, Turcotte and Tenti, 2011; Paoli, Greenfield and Reuter, 2009; Tremblay, Bouchard and Petit, 2009; Tremblay, Cusson and Morselli, 1998).

Notice also that experts' examples included both formal (e.g., law enforcement) and informal (e.g., peer judgements) sanctions [punishments]. These types of sanctions are part of social control theory, which emphasizes formal and informal mechanisms that influence individuals to conform to the rules of society, thus preventing them from committing crime (Hirschi, 1969; Sampson, 1986). Within the theory, formal mechanisms include state regulations that prevent individuals from committing criminal activities due to the fear of facing legal retributions. Informal mechanisms, on the other hand, include internalized norms and values acquired through a socialization process with peers and families that prevent an individual from committing a crime. For example, there were no peer judgments (at least clearly expressed) among the three individuals involved in the Geost scheme, the Main Entrepreneur, Developer 1 and Website Master 1, nor by any other business partners who may have been suspicious of the illicit activities happening.

The absence of these two types of sanctions is believed to influence individuals to commit online economic crime. Preventing online economic crime is often associated with increasing law enforcement capacities and skills (Bulanova-Hristova et al. 2016). Given these results, informal sanctions, such as peer judgement, could also have a prevention effect. Investigating this avenue to develop new strategies to deter individuals from participating in online economic crime could be the topic of future studies. Also, understanding why, in specific settings, peers may not judge individuals involved in such activities could be an interesting research avenue. This non-judgmentality may be related to the lack of legal opportunities mentioned above.

The third factor, ***drifting means***, refers to an encounter wherein individuals discover that participating in online economic crime is possible. Encounters mentioned by experts were multiple, including schools, online advertising platforms, or gaming activities. The drifting means factor can be interpreted as involving three steps: 1) encountering a situation or a space where individuals participated in online economic crime, 2) realizing that participating in such crime was possible, and 3) participating. Thus, the term "drifting" ties to Matza's (1990) work, which considers drifting as a state in which the tie binding self to legal expectations is broken. When one is relieved of moral restraints, crime becomes a possibility. The factor *drifting means* implies this *drift* state, but also a condition that triggers the *will* to participate in crime. I call this condition "realization" to refer to situations where individuals understand that participating in online economic crime is possible, either through their own experiences or by seeing others so doing. This recalls Matza's (1990) *preparation* condition, which states that an individual can be triggered to crime by knowing that something is possible and repeating it.

In some situations, however, experts mentioned that individuals were tricked into contributing to such crime, learning later that the work they had done was for a malicious purpose. For example, an individual is hired as a penetration tester by a group, only to learn later that he is testing the security of a company to find vulnerabilities that will then be exploited to launch ransomware on the company. This recalls Leukfeldt et al. (2020) and Bijlenga and Kleemans' (2018) argument that the neutrality of IT tasks creates a grey area that can be leveraged to successfully orchestrate criminal activities. If relevant moral restraints are still binding the individual, then the individual does not enter the drift state. Experts mentioned that often, once the line is crossed and the individuals realize that they have gotten involved in such activities, they end up continuing the said activities. Further research should investigate these processes, with research questions such as *When did you realize that you were contributing to online economic crime? Were there any hints? Why did you continue*? Unfortunately, the private chat log did not provide further information on drifting means, as the discussions did not mention how or why the individuals studied ended up spreading malicious applications.

In sum, the factor *lack of legal opportunities* justifies why individuals might be interested in online economic crime (or why online economic crime opportunities may look appealing) while the *lack of deterrents* implies a feeling of impunity as individuals do not fear informal or formal sanctions when participating in these schemes even though,

traditionally, there are sanctions. The *drifting means* factor explains how one may end up in such activities, including encounters with other individuals involved, a drift state and a realization condition. These factors are also closely linked to various criminological theories, as illustrated above. Settings where the three contextual factors converge are settings where there might be a high proportion of individuals involved in online economic crime. Studying the effect of convergence in different spaces, as well as their interplay, could be of interest for further research.

12.1.2. Money, Yet Little of it for the Masses

Interviews with experts also provided insights on what they perceived as motivators behind online economic crime. That money was the primary perceived motivation was expected, given the definition of the crime. What was startling was the general agreement that the amounts gathered, for most individuals, were not substantial. A small group of individuals -the kingpins- seemed to make large amounts of money, while the rest did not. Such discourse resembled other findings that stress inequality in revenues from criminal activities, with most individuals being quite *unsuccessful* (Paquet-Clouston, Décary-Hétu and Morselli, 2018; Levitt and Venkatesh, 2001; Tremblay and Morselli, 2000). This finding also links to a recent research on cybercrime (Collier et al., 2020) that stressed the small amounts received by individuals involved in profit-drive cybercrime, such as those providing booting services. The private chat log analysis also illustrated that those involved in spreading the Geost botnet were motivated by the idea of economic independence yet did not make as much as they expected. One individual even mentioned: *"I realized that I was led by the fact that others make good money*" (Developer 1, January 2018). Given these results, further scientific studies could focus on estimating the proportion of individuals involved in online economic crime who make large amounts of money compared to those who do not.

Experts also mentioned that feelings of pride, fame, excitement, and power over others were great motivators. These feelings were also reported as motivations by Katz (1988). However, this finding requires further assessment. Most likely, individuals behind online economic crime may have experienced these feelings, as expressed by some experts' own experiences, but to what extent this is generalized is uncertain as

motivations are intrinsic to each individual. To truly assess personal motivations, those behind online economic crime need to be surveyed.

Moreover, those spreading the Geost botnet were far from excited about their economic activities, given the adverse business environment they evolved in. Remember Developer 1 who kept on quitting the job, requiring motivational speeches from the Main Entrepreneur. This finding is, again, close to Collier et al. (2020), who interviewed individuals involved in online criminal activities and found that they were mainly lowly paid contractors who did the “invisible” work, which was or resembled legitimate work. Collier et al. (2020) even argued that focusing on the boring aspect of cybercrime (including online economic crime) and the meager revenue earned by most individuals could persuade those contemplating criminal activity to pursue legal opportunities instead.

Given the findings of Collier et al. (2020), the private chat log analysis, and the tasks surrounding online economic crime, a great proportion of individuals involved in online economic crime do not experience these feelings: they are likely involved in the crime script for monetary purposes only. Potentially, those who are motivated by pride, fame, excitement, and power end up participating in online economic crime as a byproduct of these feelings; the money is a nice additional element, but it is not the main motivator. This raises the question: online economic crime is defined as profit-driven crime (Naylor, 2003), yet for a crime to fit this definition, must profit-driven be the main motivation, or can other motivations supersede it? As long as the monetary goal is central and wealth is redistributed, then, I believe, such crime should be considered as fitting the definition of online economic crime. However, further research could look into the extent to which such feelings supersede financial motivations as well as assess who specifically experiences these feelings. Those experiencing these feelings may also be involved in specific tasks behind the crime script, such as the secondary crime of *cracking* that often surrounds online economic crime. The feeling experienced may also depend on the type of online economic crime committed, as spreading malicious applications may be less exciting than targeting a company and launching a ransomware.

The findings of this thesis also yield interesting information on the organization of those behind online economic crime. The second discussion point hence explores this, along with the role of informal workers involved at the periphery.

12.2. Organizing Online Economic Crime

The general agreement in the literature is that criminal organizations are likely to be small and loosely organized (Leukfeldt et al., 2020; Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a, b, c; Leukfeldt, 2014; Bouchard and Morselli 2014; 2007; Morselli, 2009; Morselli et al. 2007; Reuter and Haaga, 1989; Reuter, 1983). Results from the interviews, however, illustrated various forms of organization behind online economic crime, ranging from structured forms (organized criminal groups or enterprise-like groups) to organic forms (including loose networks or communities) were perceived by experts. Each is discussed below and put in relation with other studies that reported similar structures.

Structured forms included criminal groups that organize due to emergent contexts (Morselli, Turcotte and Tenti, 2011), such as large carder groups that form due to easy accessibility to information technologies, and the fall of the Soviet Union (Lusthaus and Varese, 2021). It also included depictions of traditional organized criminal groups exploiting opportunities in strategic contexts where there are criminal opportunities (Morselli, Turcotte and Tenti, 2011). The story of the group that switched from robbery to carding is a good example. Similarly, there have been several accounts in the literature of traditional organized crime groups seizing information technology economic crime opportunities or using these technologies to better conceal their activities (for reviews, see: Leukfeldt et al., 2020; Leukfeldt, Lavorgna and Kleemans, 2017; Bulanova-Hristova et al., 2016)

Structured forms also included enterprise-like organizations, where experts talked about criminal groups organized as enterprises or enterprises exploiting online economic crime opportunities. Lusthaus (2018) also argued that organizations involved in online profit-driven activities resembled firms with offices, floors and workers. In the same vein, in 2021, Böhme, Clayton and Collier published a theoretical paper that analyzed criminal entrepreneurs' decision processes behind their "profit-driven cybercrime businesses".

Organic structures were also mentioned during the interviews, including loose networks of entrepreneurs as well as communities. The former refers to entrepreneurs organizing to exploit an opportunity and then dismantling. This account is similar to findings in the traditional literature on criminal groups, which state that criminal entrepreneurs generally associate for a few economic transactions and split afterwards (Morselli, 2009; Morselli et al., 2007; Reuter and Haaga, 1989). It is also close to how offender convergence settings are conceptualized: loose and flexible networks of individuals who sometimes associate for criminal purposes (Dupont et al., 2017; Dupont et al., 2016; Holt and Smirnova 2014; Motoyama et al. 2013; Yip, Webber and Shadbolt, 2013; Holt 2013; Décary-Hétu and Dupont 2012; Christin, 2012; Holt and Lampke 2010; and many more).

Communities, on the other hand, refers to gatherings of like-minded individuals discussing various topics such as information security, hacking, and cybercrime in general and committing criminal activities together. In social science, the community concept is tied to the idea that those who form a community have a sense of solidarity, a shared identity, and follow a set of norms (Bradshaw, 2008). As an example, recall the youth gamer in one expert's story that ended up in a community on an Internet Relay Chat (IRC), building and managing botnets and stealing credit cards with a group of like-minded friends. The expert recalling this story referred to the group as a community. When studying cybercrime-related forums, a few scholars have also conceptualized online meeting places as communities (Holt and Dupont, 2019; Dupont, 2019; Afroz et al., 2013).

All in all, these perceived structures represent different angles of a complex social phenomenon: the organization of individuals involved in online economic crime. Bouchard and Morselli (2014) discussed how being involved in criminal activities is a resource pooling process, with small groups embedded in larger networks. These various structures likely depict a version of the reality of such resource pooling processes.

Which structure is reported also likely depends on the observer's perspective. For example, group of entrepreneurs, like the individuals in the private chat log, may organize around an economic crime opportunity and hire a worker to help them in their endeavors. In such a situation, their organization could be interpreted as a criminal

organization, an enterprise hiring a worker, a loose network of entrepreneurs or a community, depending on the perspective taken by the observer. Such nuance is important: it illustrates the plurality of perspectives that can be taken and how conclusions sometimes depend *more* on the observer's perspective than the structure of the organization itself.

Apart from observers' plural perspectives, the structure of criminal groups may also depend on the origin of the individuals involved, their context. This is important considering the local embeddedness of organizations involved in online economic crime (Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, 2014). Lusthaus and Varese's (2021) explanatory study also highlighted that there might be different economic and social dynamics that influence organizational structures. Bouchard and Morselli (2014) mentioned, as well, that group structures depend on the socio-legal environment in which they evolve.

Experts interviewed in this thesis came from various geographic regions and investigated groups that were established all over the world. The different structures reported may be indicative of the plurality of structures that exist and the importance of studying contexts, as highlighted by other studies (Lusthaus and Varese, 2021; Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, 2014). The three contextual factors identified above, a lack of legal opportunities, a lack of deterrents and drifting means, could be helpful in understanding why and how specific structures emerge in specific contexts.

Finally, online economic crime was defined, in this thesis, as a series of actions that lead to online illegal wealth distribution. Market transactions happening in the cybercrime industry (Lusthaus, 2018; van Wegberg et al., 2018; Hutching and Holt, 2015; Thomas et al., 2015; Moore et al., 2009) are part of the crime script, but do not define the organization behind online economic crime groups. Trading a cybercrime related product represents a secondary crime (as defined by Naylor, 2003) that can be part of an online economic crime script. This view is in line with previous research that illustrated that the various platforms on which this industry operates are offender convergence settings. Those involved in online economic crime can take advantage of them to develop their schemes: criminal expertise can be sought, co-offenders can be found, various criminally related products can be bought and sold, and even new skills

can be learned (Leukfeldt et al., 2020; Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a ,b, c; Leukfeldt, 2014).

12.2.1. Introducing the Workforce at the Periphery

To grasp the impact of a group outside of its specified boundaries, Tremblay, Bouchard and Petit (2009) brought forth the concept of economic influence. They argued that small groups can have large spheres of economic influence: their influences go beyond membership. An important finding of this thesis relates to the importance of individuals involved in online economic crime at the periphery of criminal groups. Indeed, throughout the interviews, the concept of *indispensable workers* surrounding online economic crime emerged to refer to those individuals involved in various tasks surrounding the scheme, such as transferring packages on behalf of a group, managing website servers, or laundering money. These workers are part of the sphere of economic influence of online economic crime groups. They expand the size and scope of these organizations beyond direct membership (Bouchard and Petit, 2009).

The literature on the organization of criminal groups illustrated the importance of individuals surrounding criminal groups. Facilitators are identified as individuals from the legal world who offer services to criminal groups to help in the orchestration of various criminal schemes (for a review, see Morselli and Giguère, 2006). Enablers represent individuals, not necessarily from the *legal* world, who likewise provide services to criminal groups while money mules are those who help hide financial trails (Leukfeldt et al. 2020; Leukfeldt, Kleemans and Stol, 2017a, b, c; Leukfeldt, 2014). These actors can be interpreted as *indispensable workers* or not, depending on their specific role in the criminal scheme.

This is because what the *indispensable workers* concept highlights is not the facilitating or enabling feature of these individuals in the crime orchestration. Instead, those found surrounding the crime are interpreted as *workers*: individuals engaged in or available for work. The term *worker*, as opposed to *facilitator* or *enabler*, highlights the work dependency relationship of many of these individuals to the criminal group. These workers accept the task, which usually looks legal on the surface, for money purposes. For the criminal group, who is given the task does not really matter, as long as the

worker has the skills to achieve the task, be it transferring packages, laundering money, or translating a text. The workers are indispensable as a group, yet dispensable as individuals. They are positioned at the periphery of criminal organizations, and their mass form a sphere of economic influence that those orchestrating online economic crime can exploit. One strand of indispensable workers highlighted throughout the thesis that are key to online economic crime are informal workers from the IT sector.

Informal Workers from the IT Sector

To successfully orchestrate online economic crime, IT tasks must be achieved. This may explain why a significant proportion of indispensable workers seem to come from the IT sector. Indeed, alongside findings from the private chat log involving individuals developing websites, experts reported several accounts of IT professionals being recruited to contribute to various steps leading to online economic crime. Numerous studies also mentioned groups recruiting individuals from the IT sector to orchestrate their criminal schemes (Collier et al., 2020; Bijlenga and Kleemans, 2018; Leukfeldt, Kleemans and Stol, 2017a, b, c, d;).

The informal status of these IT-related workers emerged from analyzing the private chat log: those involved in spreading the Geost botnet were conceptualized as *informal workers*[34]. The "informal" term grasps the neutrality of IT-related tasks and how the criminal character of a task can be concealed or denied, as mentioned by Leukfeldt et al. (2020) and Bijlenga and Kleemans (2018).

Informal workers are workers involved in economic activities where the products or services are not illegal per se; it is the means by which they are produced and distributed that are illegal (Castel and Portes, 1989). In the traditional literature on informal markets, informal workers engage in informal economic activities due to autonomy, social ties, ease of entry, flexibility, and freedom. Their economic activities, although informal, are also often considered socially acceptable (Ojo, Nwankwo and Gbadamosi, 2013). Similarly, the protagonists of the private chat log were engaged in such work for the sake of economic independence. Based on the conversations analyzed, the economic activities they were engaged in, whether legal, informal, or

[34] The Main Entrepreneur was conceptualized as an entrepreneur because he coordinated the development of websites. However, he was also a worker as he was working for those involved in the Geost botnet, spreading malicious applications on their behalf.

criminal, were, moreover, not condemned by any of their business partners. The term *informal* thus also nuanced the status of these IT-related workers, who do not necessarily jump from legal to criminal, but may rather evolve in a grey area.

12.3. The Double-Edged Sword: Hiring IT-Related Workers for Online Economic Crime

When looking specifically at the possibility of outsourcing IT-related tasks associated with online economic crime, one can hardly ignore the current labor platforms that gather IT-related workers. This section starts by explaining how this thesis found that these platforms open a wide array of new hiring possibilities for online economic crime groups. Then, the third discussion point is undertaken: illustrating the benefits and, more importantly, the difficulties of hiring such a workforce through digital labor platforms.

Experts interviewed mentioned that they were aware of individuals being recruited online, such as on freelancer platforms or job advertising websites. The private chat log analysis also pointed towards a digital labor platform where various services on internet marketing were traded. The Main Entrepreneur and two of his business partners participated in such a digital labor platform; using the platform to develop their economic activities allowed them to spread the Geost botnet. These findings point towards digital labor platforms representing informal spaces that can be exploited by criminal groups, and, more precisely, those behind online economic crime. In the literature, digital labor platforms are seen as unregulated spaces hosting a large workforce available at relatively low cost (Schmidt, 2017; Drahokoupil and Piasna, 2017; Drahokoupil and Fabo, 2016).

That such informal spaces can be leveraged by individuals involved in crime is in accordance with previous research: there exists an intertwined relationship between informal and criminal economies (Sabet, 2015; Vande Walle, 2008; Hagedorn, 2007). Informal economies are known to represent attractive settings for criminal groups due to their unregulated state. Informal workers are also likely to accept economic opportunities in the criminal sphere when the potential returns are good (Ojo, Nwankwo and Gbadamosi, 2013), just as the Main Entrepreneur and two of his business partners did in the private chat log. That digital labor platforms host a pool of potential workers for

online economic crime organization opens new research avenues. For example, one could explore the extent to which those behind such crime take advantage of this opportunity and which platform is favored to do so.

Such a finding may be concerning, given that, in the conventional world, digital labor platforms are reconfiguring the employer-employee relationship: hiring becomes efficient and flexible by minimizing outside employment regulations and evading company-like employment structures (Lehdonvirta, 2016). Criminal groups hiring through digital labor platforms could thus enjoy, as well, these benefits. Moreover, these platforms favor the division of jobs into microtasks (Schmidt, 2017; Drahokoupil and Piasna, 2017), which is advantageous for online economic crime groups: specific tasks can be given to workers without them being aware of the final product (Leukfeldt et al., 2020; Bijlenga and Kleemans, 2018). Subdividing the tasks is an effective way to conceal the illicit feature of the final product. Does that mean that criminal groups behind online economic crime can hire a large workforce? Well, not necessarily, as explained below.

The Challenges

Although fostering hiring flexibility, digital labor platforms do incur additional opportunity costs, especially costs for hiring informal workers. For example, Lustig et al. (2020) highlighted transaction costs resulting from hiring freelancers, both in terms of providing adequate job descriptions and managing them afterwards. Lustig et al. (2020) discussed a setting where a large technology company hired freelancers to complete specific tasks; the relationships were thus likely to happen in a professional setting.

The private chat log analysis provided information on how business relationships could take place in informal settings. Given the discussions analyzed, **the transaction costs** mentioned by Lustig (2020) seem to be **exacerbated**: the business partnerships are ephemeral and unreliable. Remember Website Master 1 mentioning to the Main Entrepreneur: "*Well probably he was writing code in his head"* when talking about the developer he hired to help with a task, illustrating the difficulties in monitoring work, and thus incurring **monitoring costs**. The same individual mentioned: "*Same story, and the programmer keeps disappearing all the time",* illustrating the additional difficulties of keeping business relationships. Goldsmith and Brewer (2015) stressed that flexible online encounters lead to **unstable relationships.** They argued that this is further

exacerbated with pseudo anonymity, allowing individuals to better conceal their identity and face few consequences when engaging and disengaging in online relationships (Goldsmith and Brewer, 2015).

The private chat log analysis also illustrated that there seemed to be high **switching costs** when a job is given to an individual. Throughout the conversations, the Main Entrepreneur was dependent on Developer 1 to continue developing the Android portals, while Developer 1 was unreliable and often stopped working. The Main Entrepreneur even mentioned once: "*Please understand it is important. And it's not an option to look for another programmer*". Rather than hiring someone else, the Main Entrepreneur made motivational speeches. All in all, these platforms may enable flexible hiring, but there may be additional costs that offset these benefits.

Reuter (1983) stated that, because employees represent a threat for entrepreneurs, criminal enterprises need **to be segmented**, thus preventing the hiring of a large workforce. The private chat log analysis illustrated that such an assumption is still relevant for those behind online economic crime. Throughout the conversations, the Main Entrepreneur acted as a **middleman** between those behind Geost and Website Master 1. Whether the Main Entrepreneur discussed with the operators or another middleman was also unclear throughout the conversations. Those behind Geost thus still segmented their operations to conceal their identity from those at the periphery, incurring additional transaction costs due to the multiplicity of actors involved.

Moreover, motivated offenders should still have incentives to conceal their identity and fragment the operations because, if workers given a licit task end up learning that it is for malicious purpose, they instantly represent a risk, as stated by Reuter (1983). However, such risk may depend on several factors, such as the geographic distance between the two parties or the extent to which the motivated offender can be blackmailed or exposed. Further research could investigate the various risks that online contracting relationships represent for motivated offenders. One interesting hypothesis that could also be investigated is: the further away in the chain from the motivated offenders who develop the scheme, the less likely people may be to conceal their identity.

On the other hand, to what extent can the maliciousness of IT-related tasks enabling online economic crime appear licit on the surface? Think of the story told by one expert of a translator who was given a task to translate a ransomware note targeting *La Gendarmerie Nationale*. A great proportion of the tasks are likely to leak the malicious purpose, so to what extent are informal workers likely to complete the tasks, disregarding their potential maliciousness? In other words, what proportion of informal workers available on digital labor platforms could drift? This leads to the fourth, and last discussion point of this thesis: presenting the workforce's limited involvement in crime-oriented platforms.

12.4. Assessing the Informal Workers' Dance

This thesis leveraged the informal workforce uncovered through the private chat analysis and developed a specific strategy to investigate its potential ties to crime-oriented spaces. To differentiate workers who talked on crime-oriented platforms, the concept of **drifter** was developed. Drifters are individuals from the informal workforce that end up discussing, at least once, in a crime-oriented space.

By posting on crime-oriented platforms, drifters are assumed to have achieved a **state of drift**: they are released from moral restraints, as defined by Matza (1990). They are not assumed to have participated in online economic crime, however. By commenting even only once, they take action in the space, which is different from lurking or simply reading on these spaces. Commenting per se is not illegal; it is only, as I argued earlier, a step that illustrates that the individual has drifted. In the drifting state, criminal activities are possible, yet not inevitable.

Of the entire workforce studied in 2017 and 2018 that respected the most liberal filtering approach, a total of **7.2%** of individuals were identified as **drifters** and they did not form a specific subpopulation, as no behavioral indicators developed could differentiate them from non-drifters. This 7.2% represents a **lower-bound** and illustrates that the online informal workforce studied encompasses workers in a state of drift, who may be willing to participate in online economic crime.

These findings are in-line with previous research: informal workers do end up seizing opportunities in criminal spheres, especially when there are higher prospects for

profit and the likelihood of getting caught is low (or criminal involvement can be denied) (Bijlenga and Kleemans, 2018; Ojo, Nwankwo and Gbadamosi, 2013; McElwee, Smith, and Somerville, 2011).

Dipping a Toe

Further investigation illustrated that drifters tend to favor informal spaces over crime-oriented ones. The drifters identified posted only a small number of comments in crime-oriented platforms (over 75% of drifters posted fewer than 10 comments according to the 2017-2018 drifter dataset). They also favored crime-oriented platforms hosted on the clearnet over those hosted on the Tor network, which has a reputation for fostering criminal activities (Faizan and Khan, 2019; Owen and Savage, 2015). This finding is in line with Sabet's (2015) study illustrating that informal workers from traditional markets preferred to avoid crime ties when possible.

The longitudinal analysis on drifters' posting behavior corroborated these results. Over time, nearly 75% of drifters who engaged in these spaces for nine years favored the informal platform over crime-oriented ones. These findings showed that **most drifters seem to dip a toe in crime-oriented spaces: their engagement is limited**. Such minimal drift recalls Matza's (1990) statement that drift is transient and rather rare for most individuals. Criminal career studies also report minimal involvement in criminal activities for most individuals (Piquero, 2004; Laub and Sampson, 2003).

Moreover, inspired by Matza's (1990) approach, this thesis did not conceptualize those posting in crime-oriented platforms as criminals who continuously break the law and are fully committed to crime. Instead, by considering drifters' posting patterns, the theoretical approach and subsequent procedure illustrated that a small proportion of the informal workers studied drifted *intermittently*. Such a nuanced approach was helpful in understanding that informal workers do not favor crime-oriented spaces. This research path could be taken by other scholars to dig further into drifters' decision process. Understanding the factors that influenced drifters to comment in and out of crime-oriented spaces could be of interest to future studies.

Those Who Drifted Permanently

The longitudinal analysis also illustrated that nearly 25% of drifters, through time, ended up posting more in crime-oriented platforms, potentially due to better economic

opportunities (Ojo, Nwankwo and Gbadamosi, 2013). However, this finding does not indicate 1) whether these drifters ended up involved in criminal activities but only drifted, and 2) whether the informal space led them to crime-oriented ones, acting as a gateway. Additional investigation is needed to answer these questions, such as what proportion are conducting criminal activities and whether the informal space has a role in their shift. Potentially, these drifters (or their activities) have specific features that can be identified to understand their drift.

These drifters are assumed to be in state of drift. **Given the large digital labor platforms that remain available, only a small proportion needs to be willing to drift.** This proportion represents those that may be targeted by organizations behind online economic crime.

Lastly, given these results, and the lack of legal economic opportunity factor mentioned by experts, a line of inquiry that could be of interest to further studies is to evaluate whether investment in the technological sector decreases participation in crime-oriented platforms. For example, experts mentioned that a growth of the cybersecurity industry in one specific region (known to be a hotbed for online economic crime) has led, recently, not only to a shortage of IT workers but also a shortage of individuals involved in online economic crime in that specific region.

12.5. Study Limits Leading to Further Research

Although this thesis provides valuable knowledge on various processes behind online economic crime, there remain several limits to the findings. These limits open new research avenues for future studies on the topic. Since several limits were mentioned throughout the chapters, this section focuses on a few important ones that are necessary to understand the limits of the work.

In the first part of the thesis, perceived motivations were assessed via experts' perspectives and my own analysis of textual data that contained discussions among individuals involved in online economic crime. A motivation is a reason someone acts a specific way; it is intrinsic to an individual. To overcome this limit, the term "perceived" motivation was used. To fully assess why individuals end up participating in online economic crime beyond financial gains, those who engage in such crime should be

interviewed. Further research should survey individuals specifically involved in online economic crime to understand their reality. Such research could evaluate whether the feelings mentioned by experts in this thesis represent motivations for those behind online economic crime or whether such feelings are rather a reflection of what experts believe would motivate them.

Another limit of this thesis lies in the cultural origin of the private chat log dataset and the two datasets related to the informal workforce. Both the private chat log and the informal platform are formed of Russian-speaking individuals. The digital labor platform is available both in English and Russian, yet most discussions happen in the Russian language. The results of this thesis in terms of experience with online economic crime as well as the relationship between informality and criminality are thus based on Russian-speaking populations. Note that “Russian-speaking” does not refer only to the Russian Federation; it encompasses a large population from various countries and different cultures, from Romania to Poland and Kazakhstan (examples are chosen randomly). Still, workers speaking other languages may be more or less inclined to participate in crime related activities. Surveying informal workers from other digital labor platforms and their potential ties to crime-oriented platforms could be the topic of future studies.

Another limit relates to identifying drifters: the results of this thesis are highly dependent on Flare System’s visibility of crime-oriented platforms. Flare Systems monitors over a hundred platforms, yet it is not necessarily focused on Russian-speaking ones, which could explain the low number of drifters found. To expand the visibility of potential crime-oriented platforms on which informal workers can drift, partnerships with other organizations could be developed.

Moreover, the name filtering approach, when identifying drifters, focuses on a perfect match approach, making the number of drifters identified a lower bound, and thus limiting the scope assessment. Although those who switch their usernames completely are not easily identifiable for researchers, individuals registering in different platforms with a slightly similar username, such as Marik9 and Marik10, could be identified. Recomputing the analysis to associate similar usernames could be done. This method would assume that similar usernames would belong to the same individual (such as Marik9 and Marik10). Although not without flaws, such a method would yield a higher lower bound.

Moreover, this thesis assesses the proportion of informal workers who drift and their relationship between informal and crime-oriented spaces through a quantitative approach. Subsequently, there was no qualitative analysis of what drifters do in crime-oriented platforms. Potentially, the drifter population is a group of individuals using crime-oriented platforms for a specific purpose that was not grasped by the analysis computed in this thesis. Further research could attempt to understand what makes individuals drift and in what kind of activities these drifters are involved in. An additional line of inquiry could also be to look at drifters' discussions on crime-oriented platforms to identify those who actively participate in online economic crime. Recomputing the Mann-Whitney U tests using only a sub-sample of drifters who are knowingly involved in online economic crime may yield different results on their distinguishability.

Finally, some studies investigated digital labor platforms and found that shady activities were hosted on them (Farooqi et al., 2017; Garg, Camp and Kanich, 2013; Motoyama et al., 2013). This endeavor was not completed in this thesis because of the length of work needed to do so. It would have required to study each comment to assess whether the topic discussed could be related to criminal activities. Investigating the platform, its categories and the various topics discussed illustrated that most of the discussions focused on legitimate inquiries about internet marketing. One subcategory hinted towards potential malicious economic activities: "*doorways and cloaking*", which refer to manipulating users into clicking on links they do not wish to. Apart from that, the platform did not embody a criminal ethos nor promoted clear criminal activities like crime-oriented platforms did. Still, upcoming research could explore various digital labor platforms to better assess the content advertised on them.

Despite these limits, this research uncovers various dynamics behind online economic crime, from contextual factors to perceived motivations to structures of organizations. It moreover assesses the role of informal workers in online economic crime and provides a first assessment of their likelihood to participate in crime-oriented platforms.

Chapter 13. **Conclusion**

Online economic crime involves a series of actions leading to illegal wealth redistribution through online means. This thesis uncovers contexts, motivations, and organizations of individuals involved in online economic crime. While doing so, it assesses the role and availability of an informal workforce surrounding the crime organization and its likelihood to participate in such criminal schemes. This was possible thanks to a mixed methodology, from inductive thematic analyses to non-parametric tests and group-based trajectory modeling.

The results are briefly summarized below. Then, **further thoughts** emerging from the results and the discussion are introduced. One idea suggests that specific geographic settings where the three identified contextual factors converge may foster large and structured organizations behind online economic crime. Another idea proposes that the uncovered informal workforce established at the periphery of online economic crime may explain the crime's reach and sophistication, along with the availability of the cybercrime industry and the incentives to target victims abroad. The existence of the informal workforce also fosters a third idea, namely, that there is a need to think beyond motivated offenders when studying online economic crime. Lastly, further thoughts on how to prevent online economic crime participation, from an informal IT worker perspective, are presented.

13.1. Thesis Results Summary

The thesis started with the objective: to uncover the contexts and motivations that may drive individuals to participate in online economic crime. Through the analyses, a confluence of contextual factors that influence individuals to participate in online economic crime was developed. They include lack of legal economic opportunities, lack of deterrents, and drifting means. These factors relate to important theoretical work in criminology, such as Merton (1968; 1938), Stafford and Warr (1993) and Matza (1990). They are also similar to what has been identified in the literature to explain the size and scope of criminal organizations (Morselli, Turcotte and Tenti, 2011; Tremblay, Bouchard and Petit, 2009; Paoli, Greenfield and Reuter, 2009; Tremblay, Cusson and Morselli, 1998). Financial gain and feelings, including pride, fame, excitement and power over

others, are also identified as motivators. Financial gain was no surprise as online economic crime is a profit-driven crime. Yet the narratives illustrated that only a small proportion of individuals are believed to end up making large amounts of money; inequality in criminal venture is a recurrent finding in the literature (Paquet-Clouston, Décary-Hétu and Morselli, 2018; Levitt and Venkatesh, 2001; Tremblay and Morselli, 2000). Feelings, on the other hand, requires further investigation given that online economic crime seems to be surrounded by boring work (Collier et al., 2020).

Experts' narratives also illustrated the various forms of organizations behind online economic crime, including structured forms (criminal groups or enterprises) and organic ones (loose networks or communities). Each of these conceptualizations most likely depicts a version of the reality; they represent different angles of the complex social phenomena that online economic crime organization represents. To further understand their prevalence, studying the origin and growth of criminal organizations beyond online settings is needed (Leukfeldt, 2014) especially given that these organizations are known to be locally embedded (Lusthaus, 2018; Leukfeldt et al., 2019; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, 2014).

Another important finding of this thesis relates to the importance of individuals involved in online economic crime at the periphery of criminal groups, the indispensable workers. The term "worker", as opposed to "facilitator" or "enabler", highlights the dependent relationship *for work* of many of these individuals to the criminal group. Within such a workforce, one that is unique to online economic crime, are informal workers involved in IT tasks, mentioned by experts and illustrated in the private chat log analysis. When looking specifically at the possibility of outsourcing IT-related tasks, one can hardly ignore the current labor platforms that gather IT-related workers, opening a wide array of new hiring possibilities for online economic crime groups.

The presence of these platforms suggests, a priori, that the possibility of hiring workers online reconfigures the employer-employee relationship discussed in Reuter (1983), allowing online economic crime organizations to hire a large workforce. However, the thesis -and previous research- also illustrated that the benefits of hiring individuals online may be mitigated by transaction costs, including hiring costs (e.g., finding the worker with the right skills), switching costs (e.g., costs associated to switching worker afterwards), and monitoring costs (e.g., making sure the job is done).

Informal workers also seem to favor informal spaces; online economic crime organization may thus sometimes have difficulty finding workers given this feature. Although not without friction, those behind online economic crime do have a large economic sphere of influence they can leverage.

The second part of the thesis focuses on understanding this workforce's relationship between informal and criminal spaces, leveraging the drifter concept. Drifters are individuals from the informal workforce that end up discussing, at least once, in a crime-oriented space, illustrating that they have entered a state of drift, as defined by Matza (1990). The objective was specifically to assess drifters' relationship between informal and crime-oriented spaces. Through various filtering techniques, drifters were estimated to form at least 7.2% of the workforce population, and no discriminatory variables differentiated drifters from non-drifters (using Mann-Whitney U tests).

Results illustrated that, for the majority of drifters, involvement in crime-oriented space was limited. The group-based trajectory model also showed that nearly 75% of them commented most often on the informal platform compared to crime-oriented ones over time. These findings suggest, similarly to Sabet (2015), that informal workers may prefer to stay in informal realms when possible. Such minimal drift also recalls Matza's (1990) statement that drift is transient and rather rare for most individuals. Nevertheless, about 25% of drifters ended up discussing only on crime-oriented platforms in the long-run. These are the ones that those behind online economic crime may try to recruit for IT tasks surrounding the scheme.

Given these findings, three further thoughts are outlined in the following sections. Hopefully, these thoughts can spark new research ideas surrounding online economic crime.

13.2. Contextual Factors and Perceived Group Structures

Previous studies have illustrated that organizations involved in economic crime related to information technologies are locally embedded (Leukfeldt et al., 2020; Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a, b, c; Leukfeldt, 2014). Leukfeldt (2014) also argued that there is a need to study the origins and growth of individuals involved in

such criminal activities. This thesis illustrated three contextual factors that may influence individuals to participate in online economic crime, regardless of their degree of involvement, as well as four perceived organizational structures. One hypothesis that comes out from these results is that in settings where the **confluence of these factors is strong, organizations behind online economic crime may be large**, in terms of active members, and more structured. Most research that concluded that the size and scope of criminal organizations were small assumed that Reuter's (1983) driving forces of product illegality were efficient: (1) contracts were not enforceable by law and (2) there were risks of arrest. Yet, in settings where the confluence of factors is strong, the second force, risks of arrest, may not be as efficient, given the lack of deterrents. Such settings may thus foster larger and more structured organizations with pre-established roles. This would explain why a variety of organizational structures were found within experts' discourse. However, organizations behind online economic crime are still unlikely to end up as large as multinational enterprises, since the forces of illegality may be strong beyond the geographic settings in which the individuals are established. Also, **additional risks and difficulties** are prevalent, given that the contracts are still not enforceable by law, as illustrated in the private chat log analysis.

Hopefully, further research will focus on understanding how geographic settings explain the prevalence and differences in the structures discussed, thus providing insightful information on the organization of criminal groups. Settings where the risk of arrest is absent provide interesting grounds for research. For example, how do criminal organizations navigate the second driving force of contracts not being enforceable by law in online environments when one of the contracting parties is abroad? Do they favor contracting individuals within their sphere of influence? Accounts of violence and threats were mentioned by a few experts, but further research on the matter is needed. Lastly, in settings where organizations behind online economic crime can grow, the organizations have the potential to involve more informal workers at the periphery to develop sophisticated schemes, as explained below.

13.3. Explaining Online Economic Crime Sophistication and Reach

Online economic crime is characterized by a long reach in terms of number of victims (Tcherni et al., 2016) and sophistication as it requires several steps to be

successful, from enticing a user to click on malicious links to hacking a network, all the way up to money laundering (Leukfeldt et al., 2019; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a, b, c, d; Leukfeldt, 2014). Based on the findings of this thesis and insights from the literature, three key elements may explain online economic crime's long reach in terms of number of victims and sophistication: 1) the possibility of leveraging an IT-related informal workforce, 2) an accessibility to offender convergence settings, and 3) the online means of the crime, which provides a diffusion capability and incentives to target individuals abroad. Each of these is discussed below.

As argued throughout this thesis, those behind online economic crime can take advantage of online digital labor platforms, which are unregulated and host a large pool of informal workers at a very low cost (Schmidt, 2017; Drahokoupil and Piasna, 2017; Drahokoupil and Fabo, 2016). If the task related to online economic crime is legal and its maliciousness can be concealed, then the pool of worker can easily be leveraged. However, if the task is clearly illegal, such as building an "evil twin" website, then those behind online economic crime will have to look for workers who are lenient towards criminality. This thesis investigated informal workers who ended up in criminal activities, likely given the adverse business environment they evolved in, and illustrated that in a large population of workers **some** will tend to drift. The sphere of economic influence of criminal groups who make use of these workers can expand significantly.

Accessibility to such a workforce is one explanation. A second one is accessibility to offender convergence settings (and the related cybercrime industry), as discussed in several studies (Leukfeldt et al., 2019; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a, b, c, d; Leukfeldt, 2014). Online meeting places can be used for market, social or learning purposes, as argued by Leukfeldt, Kleemans and Stol (2017d). These settings are a great tool for those behind online economic crime, allowing them to specialize and find the resources necessary for the orchestration of their scheme.

The third explanation is that online economic crime happens in online environments, allowing those behind such crime to target individuals in other geographical spaces than the ones they are positioned in. This process is known as a diffusion process (Llinares and Johnson, 2018; Leukfeldt and Yar, 2016; Yar, 2005). Not

only is there such a possibility, but it may also lead to less risk of arrest. Indeed, when considering Reuter's (1983) argument, where products are physically moved from one place to another, expanding geographical reach increases risk. However, in the case of online economic crime, targeting victims across geographical boundaries might be favored: it increases the level of safety of those behind such crime. As mentioned by experts, law enforcement agencies tend to investigate within their own jurisdictions and international collaborations are often slow. Thus, those behind online economic crime can target victims beyond the geographical borders they feel threatened by potential law enforcement intervention.

Given these three elements, online economic crime's long reach in terms of number of victims and sophistication may be explained. However, insights from this thesis also illustrated that hiring IT-related informal workers is not without costs. The literature also illustrates that several organizations behind online economic crime are locally embedded, and their growth depends on their social opportunity structures (Leukfeldt et al., 2020; Leukfeldt et al., 2019; Lusthaus, 2018; Leukfeldt, Lavorgna and Kleemans, 2017; Leukfeldt, Kleemans and Stol, 2017a, b, c; Leukfeldt, 2014).

Potentially, only a small number of criminal groups can successfully leverage these three elements. They are the ones responsible for highly sophisticated online economic crime that targets victims on the global scale. This would also explain why experts reported that only a small number of individuals involved in online economic crime succeeded at making large sums of money. This finding is also recurrent in the criminal achievement literature (Levitt and Venkatesh, 2001; Paquet-Clouston, Décary-Hétu and Morselli, 2018; Tremblay and Morselli, 2000).

13.4. Beyond the Concept of Motivated Offenders

The discovery of the informal workforce surrounding online economic crime and its dance between informal and crime-oriented spaces raises questions regarding the motivated offender approach currently dominating cybercrime research. Individuals involved in online economic crime or profit-driven cybercrime, regardless of their degree of involvement, are referred to as cybercriminals (Yip, Webber and Shadbolt, 2013; Yang et al., 2012; Wall, 1998) or "internet miscreants" (Caballero et al., 2011; Franklin et al., 2007). Yet there are many individuals established at the periphery of motivated

offenders organizations who are likely to contribute to the schemes, but they are not the masterminds behind the schemes. Just as the dichotomy “cyber/non-cyber” was found to be problematic when studying crime and technology (Powell, Stratton and Cameron, 2018), the “good/bad” dichotomy may be covering important dynamics at play among actors involved in online economic crime and their degree of involvement in such crime. Developing concepts that grasp this nuance is required to start understanding the complex phenomenon that is online economic crime.

Among the concepts that capture such nuances, Goldsmith and Brewer (2015) proposed *digital drift* to depict the ability of individuals to negotiate engagement boundaries in online criminal commitment. *Digital drift* grasps the flexibility, yet instability, of online criminal encounters. This concept can be useful when studying, for example, how and why informal workers end up knowingly contributing to online economic crime.

This thesis offered additional concepts to grasp the degree to which individuals may be willing to participate in criminal activities: **informal workers** and **drifters**. Informal workers refer to individuals who engage in economic activities outside of the law, but not necessarily criminal activities. **Drifters** are individuals involved in crime-oriented platforms, platforms that embody a criminal ethos (such as carding or blackhat SEO). This concept nuances that participating in crime-oriented platforms does not mean these individuals motivated offenders, but rather are “crimino-curious”. Further research could try to assess the shades of involvement, from motivated offenders to drifters, informal workers and even lurkers. This would illustrate the potential size and scope of online economic crime organizations beyond direct membership.

Finally, previous studies have associated freelancer platforms with hotbeds for criminal online activities (Farooqi et al., 2017; Motoyama et al., 2013; Garg, Camp and Kanich, 2013). These studies, however, did not consider that most of the activities they considered “black hat” or “criminal” could fall into the informal realm, which is an important contribution of this thesis. Indeed, considering the informal realm as a space where **individuals navigate between criminal, informal and legal**, while favoring to stay out of the criminal arena, can enlighten researchers on the potential realities of these workers.

13.5. Further Thoughts on Prevention

Lastly, this thesis illustrates the importance of indispensable workers and, more precisely, IT informal workers in the orchestration of online economic crime. The potential importance of digital labour platforms that gather these workers is also discussed. From these results, various strategies to deter informal IT workers from participating in online economic crime can be developed. These strategies are a first step towards moving beyond motivated offenders to prevent online economic crime.

Given the rising interest in freelance work (Schmidt, 2017; Drahokoupil and Piasna, 2017; Drahokoupil and Fabo, 2016), and that freelancers usually provide their IT services through digital labour platforms, working with the administrators of these platforms to evaluate whether workers have been solicited to participate in online economic crime would be an interesting first step. This would quantify the extent to which these platforms are used for malicious purposes beyond the results of this thesis.

Moreover, to prevent informal IT workers from contributing to online economic crime, they have to know how to detect whether the contracts they accept, and the subsequent product or service they provide, will be used for legitimate purposes. Developing programs and strategies that help informal IT workers develop skills to assess whether the work offered is for legitimate purposes or not would be useful. Also, informal IT workers not only have to know, but *they also have to care*. Thus, raising workers' awareness on the harm created by online economic crime would also be valuable.

Finally, these informal IT workers are the ones most visible, those at the end of the supply chain. They may be the ones punished or charged for their contributions in online economic crime, although they are not those who have orchestrated or thought of the scheme. Raising awareness on their vulnerable positions and the consequences they may face if they participate in online economic crime could prevent them from accepting dubious or shady work contracts.

References

Adler, F. (Ed.). (2020). *The legacy of anomie theory*. New York:Routledge.

Afroz, S., Garg, V., McCoy, D., and Greenstadt, R. (2013). Honor among thieves: A common's analysis of cybercrime economies. In *2013 APWG eCrime Researchers Summit* (pp. 1-11). IEEE. https://doi.org/10.1109/eCRS.2013.6805778

Agnew, R. (2017). Revitalizing Merton: General strain theory. In *The origins of American criminology* (pp. 137-158). Routledge.

Akdeniz, Y. (2002). Anonymity, democracy, and cyberspace. *Social Research: An International Quarterly*, *69*(1), 223-237. Retrieved June 2nd, 2021, from: https://muse.jhu.edu/article/557276/pdf

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., ... and Vasek, M. (2019). Measuring the changing cost of cybercrime. Presented at: *The 2019 Workshop on the Economics of Information Security.* Retrieved March 18, 2021, from: http://orca.cf.ac.uk/122684/

Baker, J., Lovell, K., and Harris, N. (2006). How expert are the experts? An exploration of the concept of 'expert'within Delphi panel techniques. *Nurse researcher*, *14*(1). https://doi.org/10.7748/nr2006.10.14.1.59.c6010

Baumol, W. J. (1996). Entrepreneurship: Productive, unproductive, and destructive. *Journal of business venturing*, *11*(1), 3-22. https://doi.org/10.1016/0883-9026(94)00014-X

Barratt, M. J., Ferris, J. A., and Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy*, *35*, 24-31. https://doi.org/10.1016/j.drugpo.2016.04.019

Becarria, C. (1963 [1764]). *On Crimes and Punishments*. New York: Bobbs-Merrill

Becker, H. S (2008; 1963) *Outsiders*. Simon and Schuster. New York.

Beckert, J., and Dewey, M. (2017). The social organization of illegal markets. *The architecture of illegal markets*, 1-35. https://doi.org/10.1093/oso/9780198794974.003.0001

Bernard, T. J. (1984). Control criticisms of strain theories: An assessment of theoretical and empirical adequacy. *Journal of Research in Crime and Delinquency*, *21*(4), 353-372. https://doi.org/10.1177/0022427884021004005

Bijlenga, N., and Kleemans, E. R. (2018). Criminals seeking ICT-expertise: an exploratory study of Dutch cases. *European Journal on Criminal Policy and Research*, *24*(3), 253-268. https://doi.org/10.1007/s10610-017-9356-z

Blomberg, Thomas G., et al., eds. *Delinquency and drift revisited, Volume 21: The criminology of david matza and beyond*. Routledge, 2017.

Blomberg, T. G., Cullen, F. T., Carlsson, C., and Jonson, C. L. (Eds.). (2017). *Delinquency and drift revisited, Volume 21: The criminology of david matza and beyond*. New York: Routledge.

Böhme, R., Clayton, R., and Collier, B. (2021, June). Silicon Den: Cybercrime is Entrepreneurship. In *Workshop on the Economics of Information Security (WEIS)*. Retrieved July 1st, 2021, from: https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-anderson.pdf

Bouchard, M., and Dion, C. B. (2009). Growers and facilitators: probing the role of entrepreneurs in the development of the cannabis cultivation industry. *Journal of Small Business and Entrepreneurship*, *22*(1), 25-37. https://doi.org/10.1080/08276331.2009.10593440

Bouchard, M., and Ouellet, F. (2011). Is small beautiful? The link between risks and size in illegal drug markets. *Global Crime*, *12*(1), 70-86. https://doi.org/10.1080/17440572.2011.548956

Bouchard, M., and Morselli, C. (2014). Opportunistic structures of organized crime. Paoli, L. (eds). *The Oxford handbook of organized crime*, *1*, 288-302. New York: Oxford University Press.

Bogner, A., Littig, B. and Menz, W. (2009). Introduction: Expert Interviews – An Introduction to a New Methodological DebateI. n Bogner, A., Littig, B and Menz, W. (Eds.) *Interviewing experts* (pp. 43-80). London: Palgrave Macmillan.

Bogner, A., and Menz, W. (2009). The theory-generating expert interview: epistemological interest, forms of knowledge, interaction. In Bogner, A., Littig, B and Menz, W. (Eds.) *Interviewing experts* (pp. 43-80). London: Palgrave Macmillan.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. London: Sage.

Bradshaw, T. K. (2008). The post-place community: Contributions to the debate about the definition of community. *Community Development*, *39*(1), 5-16. https://doi.org/10.1080/15575330809489738

Braun, V., and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706QP063OA

Broadhurst, R., Ball, M., and Jiang, C. J. (2020). Availability of COVID-19 related products on Tor darknet markets. *Australasian Policing*, *12*(3), 8-13.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., and Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. *An analysis of the nature of groups engaged in cyber crime, International Journal of Cyber Criminology*, *8*(1), 1-20. Retrieved June 5th, 2021, from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2461983

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in techno social networks. *Theoretical Criminology*, 10(2), 223-244. https://doi.org/10.1177/1362480606063140.

Budhathoki, N. R. (2010). *Participants' motivations to contribute geographic information in an online community* (Doctoral dissertation, University of Illinois at Urbana-Champaign).

Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M., Pool, R., de Poot, C., Werner, W., and Korsell, L. (Eds.) (2016). *Cyber-OC - scope and manifestations in selected EU member states*. Wiesbaden: Bundeskriminalamt. Retrieved February 1st, 2021, from https://bra.se/download/18.5484e1ab15ad731149e13e0d/1490082079522/2016_Cyber-oc_-_scope_and_manifestations_in_selected_eu_member_states.pd f

Caballero, J., Grier, C., Kreibich, C., and Paxson, V. (2011, August). Measuring pay-per-install: the *commoditization* of malware distribution. In *Usenix security symposium* (Vol. 13). Retrieved June 28th, 2021, from: https://www.usenix.org/legacy/events/sec11/tech/full_papers/Caballero.pdf

Cambini, C., Meccheri, N., Silvestri, V., Torino, P., Duca, C., and Pisa, U. (2011). Competition, efficiency and market structure in online digital markets. An overview and policy implications. *European Review of Industrial Economics and Policy*, *2*, 1-27. Retrieved March 15, 2021, from: http://revel.unice.fr/eriep/pdf.php?id=3212andrevue=eriep

Castells, M., and Portes, A. (1989). Underneath: The Origins, Dynamics, and Effects of the Informal Economy. Roberts et al. (eds). *The Informal Economy: Studies in Advanced and Less Developed Countries.* John Hopkins University Press: Baltimore.

Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213-224). https://doi.org/10.1145/2488388.2488408

Chu, B., Holt, T. J., and Ahn, G. J. (2010). Examining the creation, distribution, and function of malware on-line. *Department of Justice Abstract*, 1-183. Retrieved April 15, 2021, from: https://www.ojp.gov/ncjrs/virtual-library/search

Cohen, A. K. (1955). *Delinquent Boys: The Culture of the Gang*. Glencoe: The Free Press.

Cohen, L. E., and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608. https://doi.org/10.2307/2094589

Cloward, R. A., and Ohlin, L. (1960). *Delinquency and Opportunity: A Theory of* Delinquent *Gangs*. New York: The Free Press.

Collier, B., Clayton, R., Hutchings, A., and Thomas, D. (2020). Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies. Retrieved April 20th, 2021, from https://www.repository.cam.ac.uk/handle/1810/306682

Cressey, D. R. (1969). *Theft of the nation: The structure and operations of organized crime in America* (Vol. 174). Transaction Publishers.

Décary-Hétu, D., and Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160-175. https://doi.org/10.1080/17440572.2012.702523

Décary-Hétu, D. D., Morselli, C., and Leman-Langlois, S. (2012). Welcome to the scene: A study of social organization and recognition among warez hackers. *Journal of Research in Crime and Delinquency*, *49*(3), 359-382. https://doi.org/10.1177/0022427811420876

Bersnard, P. (1990). Merton in Search of Anomie. (243–54). Clark, H. Modgil, C. and Modgil, S. (eds). In *Robert K. Merton: Consensus and Controversy*. Bristol: Falmer Press

Dewey, M. (2016). *Porous borders: The study of illegal markets from a sociological perspective* (No. 16/2). MPIfG Discussion Paper. Retrieved April 1st, 2021, from: https://www.econstor.eu/handle/10419/129065

Dobson, S., Sukumar, A., and Tipi, L. (2015). Dark matters: the institutional entrepreneurship of illicit and illegal cyberspace. In *Exploring Criminal and Illegal Enterprise: New Perspectives on Research, Policy and Practice*. Emerald Group Publishing Limited.

Donaldson, L. (2001). *The contingency theory of organizations*. London: Sage.

Drahokoupil, J., and Fabo, B. (2016). The platform economy and the disruption of the employment relationship. *ETUI Research Paper-Policy Brief*, *5*. Retrieved February 1st, 2021, from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809517

Drahokoupil, J., and Piasna, A. (2017). Work in the platform economy: Beyond lower transaction costs. *Intereconomics*, *52*(6), 335-340. https://doi.org/10.1007/s10272-017-0700-9

Dupont, B. (2019). The ecology of cybercrime. Leukfeldt, R. and Holt, T. (eds) In *The human factor of cybercrime* (pp. 389-407). New York: Routledge.

Dupont, B., Côté, A. M., Boutin, J. I., and 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. https://doi.org/10.1177/0002764217734263

Dupont, B., Côté, A. M., Savine, C., and Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime*, *17*(2), 129-151. https://doi.org/10.1080/17440572.2016.1157480

Dupont, B., Côté, A. M., Boutin, J. I., and 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. https://doi.org/10.1177/0002764217734263

Eaves, Y. D. (2001). A synthesis technique for grounded theory data analysis. *Journal of advanced nursing*, *35*(5), 654-663. https://doi.org/j.1365-2648.2001.01897.x

Edwards, A., and Levi, M. (2008). Researching the organization of serious crimes. *Criminology and Criminal Justice*, *8*(4), 363-388. https://doi.org/10.1177/1748895808097403

Faizan, M., and Khan, R. A. (2019). Exploring and analyzing the dark Web: A new alchemy. *First Monday*, *24*(5). https://doi.org/10.5210/fm.v24i5.9473

Farooqi, S., Jourjon, G., Ikram, M., Kaafar, M. A., De Cristofaro, E., Shafiq, Z., ... and Zaffar, F. (2017, April). Characterizing key stakeholders in an online black-hat marketplace. In *2017 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 17-27). IEEE. https://doi.org/ 10.1109/ECRIME.2017.7945050

Featherstone, R., and Deflem, M. (2003). Anomie and strain: Context and consequences of Merton's two theories. *Sociological inquiry*, *73*(4), 471-489. https://doi.org/10.1111/1475-682X.00067

Felson, M. (2006). *The ecosystem for organized crime* (Vol. 26). Helsinki: European Institute for Crime Prevention and Control, affiliated with the United Nations. Retrieved April 2nd, 2021, from: http://old.heuni.fi/material/attachments/heuni/papers/6Ktmwqur9/HEUNI_papers_26.pdf

Fidalgo, E., Alegre, E., Fernández-Robles, L., and González-Castro, V. (2019). Classifying suspicious content in tor darknet through Semantic Attention Keypoint Filtering. *Digital Investigation*, *30*, 12-22. https://doi.org/10.1016/j.diin.2019.05.004

Furnell, S. (2003, July). Cybercrime: vandalizing the information society. In *International Conference on Web Engineering* (pp. 8-16). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45068-8_2

Franklin, J., Perrig, A., Paxson, V., and Savage, S. (2007, October). An inquiry into the nature and causes of the wealth of internet miscreants. In *ACM conference on Computer and communications security* (Vol. 10, pp. 1315245-1315292). https://doi.org/10.1145/1315245.1315292.

García, S., Erquiaga, M. J., and Shirokova (2019), Geost Botnet. the Story of the Discovery of a New Android Banking Trojan From an Opsec Error. Virus Bulletin. Retrieved April 28th, 2021, from: https://ww.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Garcia-etal.pdf

Garg, V., Camp, L. J., and Kanich, C. (2013). Analysis of ecrime in crowd-sourced labor markets: Mechanical turk vs. freelancer. In *The economics of information security and privacy* (pp. 301-321). Springer, Berlin, Heidelberg. Retrieved March 3rd, 2021, from: https://link.springer.com/content/pdf/10.1007%2F978-3-642-39498-0.pdf

Gefen, D., and Carmel, E. (2008). Is the world really flat? A look at offshoring at an online programming marketplace. *MIS quarterly*, 367-384. https://doi.org/10.2307/25148844

Goffman, E. (1983). The interaction order: American Sociological Association, 1982 presidential address. *American sociological review*, *48*(1), 1-17. https://doi.org/10.2307/2095141

Goffman E. (1981) *Forms of Talk.* Philadelphia, PA: University of Pennsylvania Press.

Goffman, E. (1974) *Frame Analysis*. Harmondsworth: Penguin

Goldsmith, A., and Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112-130. https://doi.org/10.1177/1362480614538645

Graham, M. (2013). Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities?. *The Geographical Journal, 179*(2), 177-182. https://doi.org/10.1111/geoj.12009

Graham, M., Hjorth, I., and Lehdonvirta, V. (2017). Digital labor and development: impacts of global digital labor platforms and the gig economy on worker livelihoods. *Transfer*: *European review of labor and research*, 23(2), 135-162. https://doi.org/10.1177/1024258916687250

Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. *American journal of sociology*, *91*(3), 481-510. https://doi.org/10.1086/228311

Hagedorn, J. (2007) . *Gangs in the Global City: Alternatives to Traditional Criminology*. Urbana: University of Illinois Press

Harding, P. and Jenkins, R. (1989), *Myth of the Hidden Economy*, Open University Press, Philadelphia, PA.

Haklay, M. E. (2016). Why is participation inequality important? (pp.35-45) In Capineri et al. (eds). *The European Handbook of Crowdsourced Geographic Information*. Ubiquity Press: London.

Hart, A. (2001). Mann-Whitney test is not just a test of medians: differences in spread can be important. *Bmj*, *323*(7309), 391-393. https://doi.org/10.1136/bmj.323.7309.391

Haviland, A. M., and Nagin, D. S. (2005). Causal inferences with group-based trajectory models. *Psychometrika*, *70*(3), 557-578.https://doi.org/10.1007/s11336-004-1261-y

Haythornthwaite, C., and Kendall, L. (2010). Internet and Community. *American Behavioral Scientist*, *53*(8), 1083–1094. https://doi.org/10.1177/0002764209356242

Hicks, T. (2018). Post Positivism. Frey, B.B (Ed.) *In the SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*. SAGE Publications.

Hirschi, T. (1969). Key idea: Hirschi's social bond/social control theory. *Key Ideas in Criminology and Criminal Justice,(1969)*, 55-69. Retrieved March 19th, 2021, from: https://in.sagepub.com/sites/default/files/upm-binaries/36812_5.pdf

Holloway, I., and Todres, L. (2003). The status of method: flexibility, consistency and coherence. *Qualitative research*, *3*(3), 345-357. https://doi.org/10.1177/1468794103033004

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, *31*(2), 165-177. https://doi.org/10.1177/0894439312452998

Holt, T. J., and Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40. https://doi.org/10.1080/01639625.2013.822209

Holt, T. J., and Dupont, B. (2019). Exploring the factors associated with rejection from a closed cybercrime community. *International journal of offender therapy and comparative criminology*, *63*(8), 1127-1147. https://doi.org/10.1177/0306624X18811101

Holt, T. J., Brewer, R., and Goldsmith, A. (2019). Digital drift and the “sense of injustice”: Counter-productive policing of youth cybercrime. *Deviant Behavior*, *40*(9), 1144-1156. https://doi.org/10.1080/01639625.2018.1472927

Holt, T. J., and Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, *23*(1), 33-50. https://doi.org/10.1080/14786011003634415

Holt, T. J., and Smirnova, O. (2014). *Examining the structure, organization, and processes of the international market for stolen data*. Retrieved April 17, 2021, from: https://www.ojp.gov/ncjrs/virtual-library/search

Hong, Y., and Pavlou, P. A. (2013). Online labor markets: an informal freelancer economy. *Hong, Y. and PA Pavlou (2013). Online Labor Markets: An Informal Economy. IBIT Report*. Retrieved April 17th, 2021, from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2132869

Hu, Y., Zou, F., Li, L., and Yi, P. (2020). Traffic Classification of User Behaviors in Tor, I2P, ZeroNet, Freenet. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 418-424). IEEE. https://doi.org/10.1109/TrustCom50675.2020.00064

Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., ... and McCoy, D. (2018). Tracking ransomware end-to-end. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 618-631). IEEE. https://doi.org/10.1109/SP.2018.00047

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*(1), 1-20. https://doi.org/10.1007/s10611-014-9520-z

Hutchings, A., and Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596-614. https://doi.org/10.1093/bjc/azu106

Jones, B. L., & Nagin, D. S. (2013). A note on a Stata plugin for estimating group-based trajectory models. *Sociological Methods & Research*, *42*(4), 608-613. https://doi.org/10.1177/0049124113503141

Jones, B. L., and Nagin, D. S. (2007). Advances in group-based trajectory modeling and an SAS procedure for estimating them. *Sociological methods and research*, *35*(4), 542-571. https://doi.org/10.1177/0049124106292364

Jones, B. L., Nagin, D. S., and Roeder, K. (2001). A SAS procedure based on mixture models for estimating developmental trajectories. *Sociological methods and research*, *29*(3), 374-393. https://doi.org/10.1177/0049124101029003005

Kass, R. E., and Wasserman, L. (1995). A reference Bayesian test for nested hypotheses and its relationship to the Schwarz criterion. *Journal of the American statistical association*, *90*(431), 928-934. https://doi.org/10.1080/01621459.1995.10476592

Katz, J. (1988). *Seductions of crime: Moral and sensual attractions in doing evil*. New York: Basic Books.

Kemp, S., Miró-Llinares, F., and Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(3), 293-312. https://doi.org/10.1007/s10610-020-09439-2

Kleemans, E. R. (2007). Organized crime, transit crime, and racketeering. *Crime and Justice*, *35*(1), 163-215. https://doi.org/10.1086/501509

Kleemans, E. R., and De Poot, C. J. (2008). Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology*, *5*(1), 69-98. https://doi.org/10.1177/1477370807084225

Kleemans, E. R., and Van de Bunt, H. G. (2008). Organised crime, occupations and opportunity. *Global Crime*, *9*(3), 185-197. https://doi.org/10.1080/17440570802254254

Kleemans, E. R., and Van de Bunt, H. G. (1999). The social embeddedness of organized crime. *Transnational organized crime*, *5*(1), 19-36. Retrieved April 2nd , 2021, from: https://www.researchgate.net/profile/Er-Kleemans/publication/260460230_The_social_embeddedness_of_organized_crime/links/0f3175316fc20a9ef6000000/The-social-embeddedness-of-organized-crime.pdf

Kornhauser, R. (1978). *Social Sources of Delinquency*. Chicago: University of Chicago Press.

Kozma, R. B.(2005). National Policies that Connect ICT-Based Education Reform to Economic and Social Development. *Human Technology, 1*(2), Retrieved April 2nd, 2021, from: http://www.humantechnology.jyu.fi

Krackhardt, D., and Stern, R. N. (1988). Informal networks and organizational crises: An experimental simulation. *Social psychology quarterly*, 123-140. https://doi.org/10.2307/2786835

Kshetri, N. (2010). Cloud computing in developing economies. *Computer*, *43*(10), 47-55.

Kuraku, S., and Kalla, D. (2020). Emotet Malware—A Banking Credentials Stealer. *Iosr J. Comput. Eng*, *22*, 31-41. https://doi.org/10.9790/0661-2204023140

Lehdonvirta, V. (2016) Algorithms that divide and unite: delocalization, identity, and collective action in 'microwork'. In: Flecker J (ed.) *Space, Place and Global Digital Work*. London: Palgrave-Macmillan, pp.53–80.

Levitt, S. D., and Venkatesh, S. A. (2000). An economic analysis of a drug-selling gang's finances. *The quarterly journal of economics*, *115*(3), 755-789. https://doi.org/10.1162/003355300554908

Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in organized crime*, *17*(4), 231-249. https://doi.org/10.1007/s12117-014-9229-5

Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., and Roks, R. A. (2019). Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime*, *22*(3), 324-345. https://doi.org/10.1007/s12117-019-09366-7

Leukfeldt, E. R., Kleemans, E. R., and Stol, W. P. (2017a). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology*, *57*(3), 704-722. https://doi.org/10.1093/bjc/azw009

Leukfeldt, E. R., Kleemans, E. R., and Stol, W. P. (2017b). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*, *67*(1), 39-53. https://doi.org/10.1007/s10611-016-9663-1

Leukfeldt, E. R., Kleemans, E. R., and Stol, W. P. (2017c). A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, *67*(1), 21-37. https://doi.org/10.1007/s10611-016-9662-2

Leukfeldt, R., Kleemans, E., and Stol, W. (2017d). The use of online crime markets by cybercriminal networks: A view from within. American Behavioral Scientist, 61(11), 1387-1402. https://doi.org/10.1177/0002764217734267

Leukfeldt, E. R., Kruisbergen, E. W., Kleemans, E. R., and Roks, R. A. (2020). Organized financial cybercrime: Criminal cooperation, logistic bottlenecks, and money flows. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 961-980. https://doi.org/10.1007/978-3-319-78440-3_65

Leukfeldt, E. R., Lavorgna, A., and Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, *23*(3), 287-300. https://doi.org/10.1007/s10610-016-9332-z

Leukfeldt, E. R., and Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Llinares, F., and Johnson, S. (2018). Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace. In Bruinsma, G.J.N. and Johnson S. (Eds). *The Oxford Handbook of Environmental Criminology*. Oxford: Oxford University Press, pp.1-27. https://doi.org/10.1093/oxfordhb/9780190279707.013.39

Lund, K., Coulton, P., and Wilson, A. (2011). Participation inequality in mobile location games. In *Proceedings of the 8th International Conference on Advances in Computer Entertainment Technology*. https://doi.org/10.1145/2071423.2071457

Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global crime*, *13*(2), 71-94. https://doi.org/10.1080/17440572.2012.674183

Lusthaus, J., Bruce, M., and Phair, N. (2020, September). Mapping the Geography of Cybercrime:A Review of Indices of Digital Offending by Country. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroSandPW)* (pp. 448-453). IEEE. https://doi.org/10.1109/EuroSPW51379.2020.00066

Lusthaus, J., and Varese, F. (2021). Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice*, *15*(1), 4-14. https://doi.org/10.1093/police/pax042

Lustig, C., Rintel, S., Scult, L., and Suri, S. (2020). Stuck in the middle with you: The transaction costs of corporate employees hiring freelancers. *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW1), 1-28. https://doi.org/10.1145/3392842

Matza, D. (1990). *Delinquency and drift*. New York: Routledge. https://doi.org/10.4324/9780203793596

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice*, *14*(3), 351-367. https://doi.org/10.1177/1748895813505234.

McElwee, G., Smith, R., and Somerville, P. (2011). Theorising illegal rural enterprise: is everyone at it?. Retrieved April 17th, 2021, from: https://kb.osu.edu/handle/1811/51127

McGraw, K. O., and Wong, S. P. (1992). A common language effect size statistic. *Psychological bulletin*, *111*(2), 361. https://doi.org/10.1037/0033-2909.111.2.361

Merton, R.K. (1968). *Social Theory and Social Structure*. Enlarged Editions. New York: The Free Press

Merton, R. K. (1938). *Social structure and anomie*. *American sociological review*, *3*(5), 672-682. https://doi.org/10.2307/2084686

Messner, S. F. (1988). Merton's “social structure and anomie”: The road not taken. *Deviant Behavior*, *9*(1), 33-53.

Messner, S. F., and Rosenfeld, R. (2012). *Crime and the American dream*. Wadsworth: Cengage Learning.

Miller, W. B. (2017 [1958]). *Lower class culture as a generating milieu of gang delinquency*. Routledge.

Montoya, L., Junger, M., and Hartel, P. (2013, August). How" Digital" is Traditional Crime? In *2013 European Intelligence and Security Informatics Conference* (pp. 31-37). IEEE.

Mooney, P., and Corcoran, P. (2012). Who are the contributors to OpenStreetMap and what do they do. In *Proceedings of the GIS Research UK 20th Annual Conference* (pp. 355-360). Retrieved March 3rd, 2021, from: https://www.geos.ed.ac.uk/~gisteac/proceedingsonline/GISRUK2012/Papers/presentation-87.pdf

Moore, T., Clayton, R., and Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives*, *23*(3), 3-20. https://doi.org/10.1257/jep.23.3.3

Morselli, C. (2009). *Inside criminal networks* (Vol. 8). New York: Springer.

Morselli, C., Giguère, C., and Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Social networks*, *29*(1), 143-153. https://doi.org/10.1016/j.socnet.2006.05.001

Morselli, C., Turcotte, M., and Tenti, V. (2011). The mobility of criminal groups. *Global Crime*, *12*(3), 165-188. https://doi.org/10.1080/17440572.2011.589593

Moseley, L., and Mead, D. (2001). Considerations in using the Delphi approach: design, questions and answers. *Nurse Researcher*, *8*(4), 24. Retrieved March 2nd, 2021, from: https://www.proquest.com/docview/200772951?pq-origsite=gscholarandfromopenview=true

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., and Voelker, G. M. (2011, November). An analysis of underground forums. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 71-80). https://doi.org/10.1145/2068816.2068824

Mumby, D. K., and Spitzack, C. (1983). Ideology and television news: A metaphoric analysis of political stories. *Communication Studies,* 34(3), 162-171. https://doi.org/10.1080/10510978309368137

Murray, A. (2007). *The regulation of cyberspace: control in the online environment*. Routledge-Cavendish.

Nagin, D.S. (2005). *Group-based modeling of development*. London: Harvard University Press.

Nagin, D. S. (1999). Analyzing developmental trajectories: a semiparametric, group-based approach. *Psychological methods*, *4*(2), 139. https://doi.org/10.1037/1082-989X.4.2.139

Nagin, D. S., and Land, K. C. (1993). Age, criminal careers, and population heterogeneity: Specification and estimation of a nonparametric, mixed Poisson model. *Criminology*, *31*(3), 327-362. https://doi.org/10.1111/j.1745-9125.1993.tb01133.x

Nagin, D. S., and Odgers, C. L. (2010a). Group-based trajectory modeling (nearly) two decades later. *Journal of quantitative criminology*, *26*(4), 445-453. https://doi.org/10.1007/s10940-010-9113-7

Nagin, D. S., and Odgers, C. L. (2010b). Group-based trajectory modeling in clinical research. *Annual review of clinical psychology*, *6*, 109-138. https://doi.org/10.1146/annurev.clinpsy.121208.131413

Nagin, D. S., and Piquero, A. R. (2014). Using the group-based trajectory model to study crime over the life course. In *Advancing Quantitative Methods in Criminology and Criminal Justice* (pp. 11-22). Routledge.

Nagin, D. S., and Tremblay, R. E. (2005). What has been learned from group-based trajectory modeling? Examples from physical aggression and other problem behaviors. *The Annals of the American Academy of Political and Social Science*, *602*(1), 82-117. https://doi.org/10.1177/0002716205280565

Naylor, R. T. (2003). Towards a general theory of profit-driven crimes. *British Journal of Criminology*, *43*(1), 81-101. https://doi.org/10.1093/bjc/43.1.81

Nielsen, J. (2006). Participation inequality: Encouraging more users to contribute. Nielsen Norman Group. Retrieved March 4th, 2021, from: *http://www.useit.com/alertbox/participation_inequality.html*

NVivo [Computer Software] (2021). Version 12. Retrieved from: https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home

Odinot, G., Verhoeven, M. A., Pool, R. L. D., and De Poot, C. J. (2017). Organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement. Retrieved January 10th, 2021, from: https://research.hva.nl/en/publications/organised-cybercrime-in-the-netherlands-empirical-findings-and-im

Ojo, S., Nwankwo, S., and Gbadamosi, A. (2013). Ethnic entrepreneurship: the myths of informal and illegal enterprises in the UK. *Entrepreneurship and Regional Development*, *25*(7-8), 587-611. https://doi.org/10.1080/08985626.2013.814717

Ouellet, F. (2019). Stop and go: Explaining the timing of intermittency in criminal careers. *Crime and Delinquency*, *65*(5), 630-656. https://doi.org/10.1177/0011128717753114

Owen, G., and Savage, N. (2015). The Tor dark net. Global Commission on Internet Governance Paper Series. GCIG Paper No. 20. 20p. Available at: https://www.cigionline.org/static/documents/no20_0.pdf

Paoli, L. (2007). Mafia and organised crime in Italy: the unacknowledged successes of law enforcement. *West European Politics*, *30*(4), 854-880. https://doi.org/10.1080/01402380701500330

Paoli, L., Greenfield, V. A., and Reuter, P. (2009). *The world heroin market: Can supply be cut?*. New York: Sage.

Paquet-Clouston, M., Décary-Hétu, D., and Morselli, C. (2018). Assessing market competition and vendors' size and scope on AlphaBay. *International Journal of Drug Policy*, *54*, 87-98. https://doi.org/10.1016/j.drugpo.2018.01.003

Paquet-Clouston, M., Haslhofer, B., and Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, *5*(1), https://doi.org/10.1093/cybsec/tyz003

Passas, N. (2000). Global anomie, dysnomie, and economic crime: Hidden consequences of neoliberalism and globalization in Russia and around the world. *Social Justice*, *27*(2 (80), 16-44. Retrieved July 12th, 2021, from: https://www.jstor.org/stable/29767205

Patton, M. Q. (2005). Qualitative research. In *Encyclopedia of statistics in behavioral science*. Chichester: Wiley.

Paternoster, R., and Piquero, A. (1995). Reconceptualizing deterrence: An empirical test of personal and vicarious experiences. *Journal of Research in Crime and Delinquency*, *32*(3), 251-286. https://doi.org/10.1177/0022427895032003001

Perito, D., Castelluccia, C., Kaafar, M. A., and Manils, P. (2011, July). How unique and traceable are usernames?. In *International Symposium on Privacy Enhancing Technologies Symposium* (pp. 1-17). Springer, Berlin, Heidelberg.

Piquero, A. R. (2004). Somewhere between persistence and desistance: The intermittency of criminal careers. In S. Maruna and R. Immarigeon (eds.) In *After crime and punishment: Pathways to offender reintegration*. Portland: Willan Publishing

Piquero, A., and Paternoster, R. (1998). An application of Stafford and Warr's reconceptualization of deterrence to drinking and driving. *Journal of research in crime and delinquency*, *35*(1), 3-39. https://doi.org/10.1177/0022427898035001001

Piquero, A. R., and Pogarsky, G. (2002). Beyond Stafford and Warr's reconceptualization of deterrence: Personal and vicarious experiences, impulsivity, and offending behavior. *Journal of research in crime and delinquency*, *39*(2), 153-186. https://doi.org/10.1177/002242780203900202

Pittaro, M. L. (2007). Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology*, *1*(2), 180-197. Retrieved February 28th, 2021, from: http://cybercrimejournal.com/mpittarojccjuly2007.pdf

Ponsaers, P., Shapland, J. and Williams, C.C. (2008), "Does the informal economy link to organised crime?", *International Journal of Social Economics*, 35(9), 644-650. https://doi.org/10.1108/03068290810896262

Portes, A. and Haller, W. (2010). The Informal Economy. In N. Smelser and R. Swedberg (eds.), *The Handbook of Economic Sociology* (pp. 403-426). Princeton: Princeton University Press. https://doi.org/10.1515/9781400835584.403

Powell, A., Stratton, G., and Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. New York: Routledge.

Rajaraman, V. (2018). *Introduction to information Technology*. Delhi, India: PHI Learning Pvt. Ltd.

Rangaswamy, N. (2019). A note on informal economy and ICT. *The Electronic Journal of Information Systems in Developing Countries*, *85*(3), e12083. https://doi.org/10.1002/isd2.12083

Rege, A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology*, *3*(2). Retrieved June 29th, 2021, from: https://www.cybercrimejournal.com/AunshulIJCCJuly2009.pdf

Reuter, P. (1983). *Disorganized Crime: Illegal Markets and the Mafia*. Cambridge: MIT Press.

Reuter, P., and Haaga, J. (1989). The organization of high-level drug markets: An exploratory study. Retrieved April 17th, 2021, from: https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=111511

Roach, S.S. (2004). *More Jobs, Worse Work*. the New York Times, Retrieved April 28th, 2021, from http://www.nytimes.com/2004/2007/2022/opinion/more-jobs-worse-work.html

Rosenfeld, R. (1989). Robert Merton's contributions to the sociology of deviance. *Sociological Inquiry*, *59*(4), 453-466. https://doi.org/10.1111/j.1475-682X.1989.tb00120.x

Roulston, K. (2001). Data analysis and 'theorizing as ideology'. *Qualitative research*, *1*(3), 279-302. https://doi.org/10.1177/146879410100100302

Sabet, D. M. (2015). Informality, Illegality, and Criminality in Mexico's Border Communities. *Journal of Borderlands Studies*, *30*(4), 505-517. https://doi.org/10.1080/08865655.2015.1101704

Sabet, J., and Fabo, B. (2016). The platform economy and the disruption of the employment relationship. *European Trade Union Institute Research Paper-Policy Brief*, *5*. Retrieved March 3rd, 2021, from: https://www.etui.org/publications/policy-briefs/european-economic-employment-and-social-policy/the-platform-economy-and-the-disruption-of-the-employment-relationship

Sampson, R. J. (1986). Crime in cities: The effects of formal and informal social control. *Crime and justice*, *8*, 271-311. https://doi.org/10.1086/449125

Sampson, R. J., and Laub, J. H. (2003). Life-course desisters? Trajectories of crime among delinquent boys followed to age 70. *Criminology*, *41*(3), 555-592. https://doi.org/10.1111/j.1745-9125.2003.tb00997.x

Schmidt, F. A. (2017). Digital labor markets in the platform economy. *Mapping the Political Challenges of Crowd Work and Gig Work*, Friedrich-Ebert-Stiftung. Retrieved March 4th, 2021, from: http://www.bollettinoadapt.it/wp-content/uploads/2020/10/13164.pdf

ScipyStats [Computer Software] (2021). Retrieved March 15th, 2021, from: https://docs.scipy.org/doc/scipy/reference/generated/scipy.stats.mannwhitneyu.html

Sembera, V. Paquet-Clouston, M. Garcia, S. and Erquiaga, MJ. (accepted) Cybercrime Specialization: An Exposé of a Malicious Android Obfuscation-as-a-Service. *3rd Workshop on Attackers and Cyber-Crime Operations. IEEE European Symposium on Security and Privacy 2021*.

Shanteau, J. (1989). Psychological characteristics and strategies of expert decision makers. In B. Rohrmann, L. R. Beach, C. Vlek, and S. R. Watson (Eds.), *Advances in decision research* (pp. 203-215). Amsterdam: North Holland

Shapland, J. (2004). *The informal economy: Threat and opportunity in the city*. Edition Iuscrim (open library) . Retrieved March 15th, 2021, from: https://pure.mpg.de/rest/items/item_3014458/component/file_3014459/content

Shier, R. (2004). The mann-whitney u test. *Mathematics Learning Support Centre [Internet].* Retrieved January 16th, 2021, from https://www.lboro.ac.uk/media/wwwlboroacuk/content/mlsc/downloads/2.3_mann_whitney.pdf

Sitren, A. H., and Applegate, B. K. (2012). Testing deterrence theory with offenders: The empirical validity of Stafford and Warr's model. *Deviant Behavior*, *33*(6), 492-506. https://doi.org/10.1080/01639625.2011.636685

Sitren, A. H., and Applegate, B. K. (2007). Testing the deterrent effects of personal and vicarious experience with punishment and punishment avoidance. *Deviant Behavior*, *28*(1), 29-55. https://doi.org/10.1080/01639620600887261

Smith, R., Grabosky, P., and Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters*, *58*(1), 22-23. https://doi.org/10.1080/09627250408553240

Soudijn, M. R., and Zegers, B. C. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in organized crime*, *15*(2-3), 111-129. https://doi.org/10.1007/s12117-012-9159-z

Stafford, M. C., and Warr, M. (1993). A reconceptualization of general and specific deterrence. *Journal of research in crime and delinquency*, *30*(2), 123-135. https://doi.org/10.1177/0022427893030002001

Statista Research Department (2021). Number of freelance workers in the United States from 2014 to 2020. Retrieved June 7th, 2021, from: https://www.statista.com/statistics/685468/amount-of-people-freelancing-us/#:~:text=In%202019%2C%20there%20were%2057,freelance%20work%20in%20the%20U.S.

STATA [Computer Software] (2021). Version 16. Retrieved from: https://www.statalist.org/

Statosphere (2021). Stratosphere Research Laboratory. https://www.stratosphereips.org/

Strauss, K. (2018a). Precarious work and winner-take-all economies. Gordon, L. et al. (eds) In *The new Oxford handbook of economic geography*. https://doi.org/10.1093/oxfordhb/9780198755609.013.22

Strauss, K. (2018b). Precarious Work. R., Douglas et al. (eds). In *The International Encyclopedia of Geography*. John Wiley & Son. https://doi.org/10.1002/9781118786352.wbieg0718.pub2

Sun, N., Rau, P. P. L. and Ma, L. (2014). Understanding lurkers in online communities: A literature review. Computers in Human Behavior, 38, 110-117. https://doi.org/10.1016/j.chb.2014.05.022

Sykes, G. M., and Matza, D. (2017). Techniques of neutralization: A theory of delinquency. In *Delinquency and drift revisited* (pp. 33-41). New York: Routledge.

Tanczer, L. M. (2019). 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers. *Contemporary Security Policy, 1–21.* https://doi.org/10.1080/13523260.2019.1669336

Tcherni, M., Davies, A., Lopes, G., and Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave?. *Justice Quarterly*, *33*(5), 890-911. https://doi.org/10.1080/07418825.2014.994658

Thomas, K., Huang, D., Wang, D., Bursztein, E., Grier, C., Holt, T. J., ... and Vigna, G. (2015). Framing dependencies introduced by underground commoditization. Workshop on the Economics of Information Security. Retrieved April 28, 2021, from: https://research.google/pubs/pub43798

Tremblay, P., Bouchard, M., and Petit, S. (2009). The size and influence of a criminal organization: A criminal achievement perspective. *Global Crime*, *10*(1-2), 24-40. https://doi.org/10.1080/17440570902782428

Tremblay, P., Cusson, M., and Morselli, C. (1998). Market offenses and limits to growth. *Crime, Law and Social Change*, *29*(4), 311-330. https://doi.org/10.1023/A:100822490080.

Tremblay, P., and Morselli, C. (2000). Patterns in Criminal Achievement: Wilson and Abrahamse Revisited. *Criminology, 38(2), 633–657.* https://doi.org/10.1111/j.1745-9125.2000.tb00901.x

Valeros, V. and Garcia, S. (2021, submitted). Online Marketing Forums as Safe Heavens for Shady Services. *3rd Workshop on Attackers and Cyber-Crime Operations.* IEEE European Symposium on Security and Privacy 2021.

Vande Walle, G. (2008), A matrix approach to informal markets: towards a dynamic conceptualisation, *International Journal of Social Economics*. 35(9), 651-665. https://doi.org/10.1108/03068290810896271

Van Mierlo, T. (2014). The 1% rule in four digital health social networks: an observational study. *Journal of medical Internet research*, *16*(2), e33. https://doi.org/10.2196/jmir.2966

Van Reenen, J., Bloom, N., Draca, M., Kretschmer, T., Sadun, R., Overman, H., and Schankerman, M. (2010). *The economic impact of ICT*. Final report. Retrieved March 20th, 2021, from: http://bruegel.org/wp-content/uploads/imported/events/LT_26_April_Invitation.pdf

Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganan, C. H., Klievink, B., ... and Van Eeten, M. (2018). Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In *27th {USENIX} security symposium ({USENIX} security 18)* (pp. 1009-1026). Retrieved November 18th, 2020, from: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-van_wegberg.pdf

Virus Total (2020). VirusTotal. https://www.virustotal.com/gui/

Von Lampe, K. (2008). Organized crime in Europe: conceptions and realities. *Policing: A Journal of Policy and Practice*, *2*(1), 7-17. https://doi.org/10.1093/police/pan015

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Cambridge: Polity.

Wall, D. S. (1998). Catching cybercriminals: policing the Internet. *International Review of Law, Computers and* Technology, *12*(2), 201-218. https://doi.org/10.1080/13600869855397

Wang, Y., Liu, T., Tan, Q., Shi, J., and Guo, L. (2016). Identifying users across different sites using usernames. *Procedia Computer Science*, *80*, 376-385. https://doi.org/10.1016/j.procs.2016.05.336

Watt, D. (2007). On becoming a qualitative researcher: the value of reflexivity. *Qualitative Report*, *12*(1), 82-101. Retrieved January 16th, from: https://files.eric.ed.gov/fulltext/EJ800164.pdf

Williamson, O. E. (1993). Transaction cost economics and organization theory. *Industrial and corporate change*, *2*(2), 107-156. https://doi.org/10.1093/icc/2.2.107

Wood, H. (2014). The long tail of OpenStreetMap. Retrieved March 4th, 2021 from: http://harrywood.co.uk/blog/2014/11/17/the-long-tail-of-openstreetmap/#slide18

Yang, C., Harkreader, R., Zhang, J., Shin, S., and Gu, G. (2012). Analyzing spammers' social networks *for* fun and profit: a case study of cyber criminal ecosystem on twitter. In *Proceedings of the 21st international conference on World Wide Web* (pp. 71-80). Retrieved June 28th, 2021, from: https://people.engr.tamu.edu/guofei/paper/CyberEco_WWW12.pdf

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427. https://doi.org/10.1177/147737080556056

Yip, M., Webber, C., and Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516-539. https://doi.org/10.1080/10439463.2013.780227

Zang, E., and Max, J. T. (2020). Bayesian estimation and model selection in group-based trajectory models. *Psychological Methods*. http://dx.doi.org/10.2139/ssrn.3315029

Appendix A. Consent Form

Consent Form for Research Participation

Principal Investigator: Masarah-Cynthia Paquet-Clouston, PhD Student in Criminology, and part-time Security Researcher at GoSecure
PhD Student Supervisor: Prof. Martin Bouchard
Research Collaborators: (i) Sebastian Garcia: Assistant Professor at CTU University, PhD. Director of Stratosphere Laboratory; (ii) Marìa José Erquiaga, Licence Professionnelle, Researcher, Team Leader of the Aposemat project, part of the Stratosphere Laboratory; (iii) Anna Shirokova, Researcher at Avast Software (iv) Veronica Valeros: MSc. Technical Leader of Stratosphere Laborator

Invitation and Study Purpose
You are being invited to contribute, through an interview, to a research that aims at understanding the incentives behind criminal opportunities exploitations related to information technologies.

> **Title:** Beyond "Cyber": Exploring the Incentives behind Criminal Opportunities Exploitations related to Information Technologies
>
> **Thesis Summary:** This study aims at understanding w*hat are the personal and contextual factors that influence one's decisions to exploit IT-related criminal opportunities, such as writing malware?* To do so, we aim to (Goal 1.) get the point of view of those behind the malicious activities and examine their decision-making processes when exploiting ITs-related criminal opportunities and (Goal 2.) understand the contextual factors that may influence one to exploit IT-related criminal opportunities. To answer the study's objective, we dive into the technical structure of a botnet named *Geost*. The malicious scheme behind the *Geost* botnet is as follows: through hacked phone applications advertised on Russian websites, the operators own a network of infected phones. Based on this, we attempt at understanding the backgrounds and motivations of those involved in developing the malicious software with the use of data available online on public forums and a leaked and publicly available chat log of one of the main operators. Then, we move to comprehend the contextual factors (i.e. social, cultural, economic, political) that may influence individuals to develop such malicious software by discussing with cybersecurity experts from the same geographical region as the *Geost* operators and/or actively involved in stopping similar malicious schemes.
>
> **Interview context:** This interview is conducted for Masarah-Cynthia Paquet-Clouston's PhD thesis, as well as for research about the *Geost* botnet, led by the Stratosphere Research group, based at the Czech Technical University, in collaboration with Avast (a Czech anti-virus company) and GoSecure (an American cybersecurity company with offices in Canada).

Interview Procedures

Interviewer: Masarah-Cynthia Paquet-Clouston

Observers: Two of the collaborators, Sebastian Garcia and Maria José Erquiaga, may sit in the interview, if the research participant is comfortable with this.

Interviewee: A cybersecurity expert from the same geographical region as the *Geost* operators and/or actively involved in stopping similar malicious schemes

Objective: Understand the contextual factors (i.e., social, cultural, economic, political) that may influence one to exploit criminal opportunities related to information technologies

Location: Online

Time: between one hour to one hour and half

Confidentiality

All interviews are anonymous: any identifiable information, such as your name, professional occupation or company, will not be disclosed anywhere in the research. We will only keep the country from which you are operating as a cybersecurity expert. The interview will be recorded only with your acceptance. Once the interview's transcription will be completed, all identifiable information will be removed, and if there is a recording, it will be destroyed.

Potential Risks of the Study

There are no foreseeable risks to you in participating in this study. If you think of any, please let me know.

Potential benefits

Your participation in the study will help us develop knowledge on contextual factors that may influence one to develop malicious software.

Withdrawal

You can withdraw from the study at any time during the interview and after the interview without giving any reasons. If you wish to withdraw after the interview, you can write to the email address to: […] and I will delete your interview transcript immediately and will not consider the interview in the study's results.

Study's Results

The study's results will be presented at international conferences in cybersecurity, published in scientific articles and my final PhD thesis. ***If you wish to receive the study's result personally, let me know (during or after the interview) and I will send them by email once completed.***

Data Stewardship

The data will be kept by myself on a password protected external disk for five years following the publication of the research. All collaborators cited above will be able to access the disk strictly for the study. If the data is requested by an external party, it will be given only under official legal requirements.

Contact Information
If you have any questions, you can contact me, Masarah Paquet-Clouston, at the email address: […] or call me at […].

Contact for Complaints
If you have any concerns about your rights, as a research participant and/or your experiences while participating in this study, you may contact Dr. Jeffrey Toward, Director, Office of Research Ethics […] or […].

Thank you for your collaboration!

Appendix B. Crime-Oriented Platforms

Forum Name	Hosted	Type	N. Actors	N. Comments
Nulled to	Clearnet	Cracking and Leaks	415	3205
Dark Money	Darknet	Money Laundering	287	4872
Best Hack Forum	Clearnet	Hacking	232	6311
Exploit in	Clearnet	Hacking	147	5845
Black Hat World	Clearnet	Black hat SEO	141	2319
Club2crd	Clearnet	Carding	113	2407
RaidForums	Clearnet	Cracking and Leaks	93	488
Cracked	Clearnet	Cracking and Leaks	86	1212
Cracking pro	Clearnet	Cracking and Leaks	84	482
Dread	Darknet	Discussions, Sales, Questions	83	1207
Hidden answer	Darknet	Discussions, Sales, Questions	45	187
Xss is	Darknet	Hacking	43	538
Prtship	Clearnet	Carding	42	383
Cracking King	Clearnet	Cracking and Leaks	39	73
Torum forum	Darknet	Discussions, Sales, Questions	36	202
Trollodrome2	Darknet	Discussions, Sales, Questions	34	90
French deep web forum	Darknet	Discussions, Sales, Questions	30	138
Rutor	Darknet	Cryptomarket	29	93
Sinister	Clearnet	Cracking and Leaks	28	738
DNMAvengers	Darknet	Cryptomarket	26	280
Dream forum	Darknet	Discussions, Sales, Questions	24	94
The Hub	Darknet	Discussions, Sales, Questions	15	78
SatForum	Darknet	Carding	12	1480
International Carding Alliance	Clearnet	Carding	9	15
Deutschland	Clearnet	Discussions, Sales, Questions	7	66
Verified Carders	Darknet	Carding	7	32
Envoy Forum	Darknet	Discussions, Sales, Questions	7	13
Onion Land	Darknet	Discussions, Sales, Questions	7	44
Wall Street forum	Darknet	Cryptomarket	5	27
Dark Anti French System (DFAS)	Darknet	Discussions, Sales, Questions	5	104
Criminality French Market	Darknet	Discussions, Sales, Questions	3	12
Xaker26	Clearnet	Hacking	2	46
CardVilla	Clearnet	Carding	2	2
Sinfulsite	Clearnet	Cracking and Leaks	1	2
Hermes	Darknet	Discussions, Sales, Questions	1	1
Main Helium	Darknet	Hacking	1	5
CryptBB	Darknet	Hacking	1	5
GreySec	Clearnet	Hacking	1	1

Appendix C. Additional Mann-Whitney U Tests

Time Filter 1 (TF1): From 2015 to 2020
Name Filter 1 (NF1): Minimum of five characters in username

Table 1
Entire Platform Population TF1 and NF1

	Drifters N= 1,557			Non-Drifters N=21,791			Statistics		
	Mean	Std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	34.76	171.77	4.0	28.87	149.23	4.0	15875519	0.0000	0.53
N. days active	16.24	44.15	3.0	13.44	40.40	2.0	15666700	0.0000	0.54
Diversification									
SDI	0.33	0.40	0.0	0.29	0.39	0.0	15996351	0.0000	0.53
N. cat.	2.13	1.81	1.0	1.97	1.68	1.0	16007108	0.0000	0.53
N. sub-cat	3.55	6.07	1.0	3.14	5.34	1.0	16029862	0.0000	0.53
Business									
N. $ sign	1.50	12.87	0.0	1.02	10.54	0.0	16134200	0.0000	0.54
Prop. $ sign	0.04	0.13	0.0	0.04	0.13	0.0	16153262	0.0000	0.52
Specific Topics									
Search Engine	3.00	17.75	0.0	2.94	21.36	0.0	16895351	0.3573	0.50
Monetizing sites	7.50	80.50	0.0	5.65	37.24	0.0	16849367	0.2950	0.50
Practical opt.	3.82	19.08	0.0	3.81	31.76	0.0	16959295	0.4905	0.50
Comm. of prof.	6.52	50.43	0.0	3.89	40.65	0.0	16104023	0.0000	0.53
Site building	4.75	26.53	0.0	4.62	45.83	0.0	16227874	0.0002	0.52
Exch. and sale	1.61	8.10	0.0	1.45	9.62	0.0	16307064	0.0001	0.52
Purch. traffic	0.93	10.68	0.0	0.66	9.76	0.0	16832449	0.1637	0.50
Work web master	0.97	4.94	0.0	0.96	6.04	0.0	16778840	0.1291	0.50
Not about work	5.66	59.09	0.0	4.89	71.32	0.0	16548104	0.0020	0.51

Table 2
Top 30% TF1 and NF1

	Drifters N= 510			Non-Drifters N=6,414			Statistics		
	Mean	Std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	99.79	289.63	29.0	91.10	264.88	27.0	1559642	0.04	0.52
N. days active	44.68	68.89	19.0	40.36	67.16	17.0	1526452	0.01	0.53
Diversification									
SDI	0.52	0.35	0.6	0.51	0.36	0.6	1617283	0.34	0.51
N. cat.	3.69	2.33	3.0	3.53	2.25	3.0	1577524	0.09	0.52
N. sub-cat	7.70	9.23	5.0	7.19	8.47	4.0	1598917	0.20	0.51
Business									
N. $ sign	4.29	22.23	0.0	3.22	19.25	0.0	1536479	0.01	0.53
Prop. $ sign	0.04	0.08	0.0	0.04	0.08	0.0	1552542	0.02	0.53
Specific Topics									
Search Engine	8.64	30.23	0.0	9.29	38.61	0.0	1619719	0.34	0.50
Monetizing sites	21.73	139.65	1.0	17.80	67.07	1.0	1629106	0.44	0.50
Practical opt.	10.81	32.21	1.0	11.73	57.74	1.0	1595856	0.17	0.51
Comm. of prof.	19.06	86.82	0.0	12.47	74.21	0.0	1515778	0.00	0.54
Site building	13.28	45.15	1.0	14.52	83.63	1.0	1579436	0.08	0.52
Exch. and sale	4.18	13.72	0.0	4.21	17.37	0.0	1587799	0.10	0.51
Purch. traffic	2.54	18.54	0.0	1.92	17.90	0.0	1626877	0.39	0.50
Work web master	2.45	8.36	0.0	2.72	10.86	0.0	1615643	0.28	0.51
Not about work	17.11	102.36	0.0	16.43	130.75	0.0	1561045	0.02	0.52

Time Filter 1 (TF1) : From 2015 to 2020
Name Filter 2 (NF2): Minimum of six characters in usernames

Table 3
Entire Platform Population TF1 and NF2

	Drifters N= 1,234			Non-Drifters N=22,114			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	30.74	163.49	4.0	29.18	150.1	4.0	13051649	0.0046	0.52
N. days active	15.24	42.76	3.0	13.54	40.54	2.0	12921421	0.0007	0.53
Diversification									
SDI	0.32	0.40	0.0	0.29	0.39	0.0	13023474	0.0011	0.52
N. cat.	2.09	1.79	1.0	1.97	1.68	1.0	13093770	0.0032	0.52
N. sub-cat	3.44	5.99	1.0	3.16	5.36	1.0	131827401	0.0136	0.52
Business									
N. $ sign	1.44	13.82	0.0	1.03	10.51	0.0	13094995	0.0002	0.52
Prop. $ sign	0.04	0.13	0.0	0.04	0.13	0.0	13102302	0.0003	0.52
Specific Topics									
Search Engine	2.59	13.49	0.0	2.96	21.48	0.0	13499189	0.1953	0.51
Monetizing sites	7.55	88.34	0.0	5.68	37.25	0.0	13584526	0.3772	0.50
Practical opt.	3.64	19.20	0.0	3.82	31.60	0.0	13516339	0.2482	0.50
Comm. of prof.	5.08	35.97	0.0	4.01	41.66	0.0	13123717	0.0012	0.52
Site building	4.49	26.69	0.0	4.64	45.60	0.0	13209078	0.0102	0.52
Exch. and sale	1.67	8.69	0.0	1.45	9.58	0.0	13152484	0.0011	0.52
Purch. traffic	0.70	7.16	0.0	0.67	9.95	0.0	13487232	0.0965	0.51
Work web master	1.05	5.35	0.0	0.96	6.01	0.0	13430183	0.0727	0.51
Not about work	3.96	48.54	0.0	5.00	71.60	0.0	13395992	0.0274	0.51

Table 4
Top 30% TF1 and NF2

	Drifters N= 395			Non-Drifters N= 6,529			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	89.67	280.21	29.00	91.87	265.96	27.0	1246473	0.13	0.52
N. days active	42.70	67.85	18.00	40.56	67.27	17.0	1223830	0.04	0.53
Diversification									
SDI	0.51	0.35	0.59	0.51	0.36	0.6	1285253	0.46	0.50
N. cat.	3.65	2.35	3.00	3.53	2.25	3.0	1262927	0.24	0.51
N. sub-cat	7.53	9.26	4.00	7.21	8.48	4.0	1283097	0.43	0.50
Business									
N. $ sign	4.23	24.21	0.00	3.25	19.16	0.0	1216474	0.02	0.53
Prop. $ sign	0.04	0.09	0.00	0.04	0.08	0.0	1219649	0.02	0.53
Specific Topics									
Search Engine	7.59	23.05	0.00	9.34	38.77	0.0	1273839	0.33	0.51
Monetizing sites	22.40	155.21	1.00	17.83	66.98	1.0	1282424	0.42	0.50
Practical opt.	10.55	32.87	1.00	11.73	57.37	1.0	1268434	0.28	0.51
Comm. of prof.	15.10	62.44	0.00	12.82	75.93	0.0	1202405	0.01	0.53
Site building	12.81	46.07	1.00	14.53	83.08	1.0	1263020	0.23	0.51
Exch. and sale	4.43	14.92	0.00	4.20	17.25	0.0	1250178	0.12	0.52
Purch. traffic	1.86	12.55	0.00	1.98	18.22	0.0	1288007	0.48	0.50
Work web master	2.73	9.15	0.00	2.70	10.78	0.0	1286803	0.46	0.50
Not about work	12.21	85.27	0.00	16.74	131.04	0.0	1249680	0.10	0.52

Time Filter 1 (TF1) : From 2015 to 2020
Name Filter 3 (NF3): Minimum of five characters AND at least an uppercase OR a number OR one special character in usernames

Table 5
Entire Platform Population TF1 and NF3

	Drifters N= 946			Non-Drifters N= 22,402			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	30.02	119.77	5.0	29.23	152.01	4.0	9643767	0.0000	0.54
N. days active	15.08	34.68	3.0	13.56	40.90	2.0	9512654	0.0000	0.55
Diversification									
SDI	0.33	0.40	0.0	0.29	0.39	0.0	9957233	0.0002	0.53
N. cat.	2.16	1.82	1.0	1.97	1.68	1.0	9908008	0.0000	0.53
N. sub-cat	3.51	5.68	1.0	3.16	5.38	1.0	9990163	0.0005	0.53
Business									
N. $ sign	1.10	4.71	0.0	1.05	10.90	0.0	10040786	0.0000	0.53
Prop. $ sign	0.04	0.14	0.0	0.04	0.13	0.0	10058989	0.0000	0.53
Specific Topics									
Search Engine	2.36	13.01	0.0	2.96	21.41	0.0	10532269	0.3341	0.50
Monetizing sites	6.27	29.05	0.0	5.75	42.00	0.0	10381182	0.1011	0.51
Practical opt.	3.08	12.15	0.0	3.85	31.62	0.0	10479627	0.2412	0.51
Comm. of prof.	6.85	54.34	0.0	3.94	40.73	0.0	9887739	0.0000	0.53
Site building	3.83	17.13	0.0	4.66	45.60	0.0	10129655	0.0024	0.52
Exch. and sale	1.40	5.68	0.0	1.46	9.66	0.0	10070740	0.0001	0.52
Purch. traffic	0.65	6.04	0.0	0.68	9.95	0.0	10452972	0.0891	0.51
Work web master	0.93	4.91	0.0	0.96	6.02	0.0	10549088	0.3583	0.50
Not about work	4.67	47.23	0.0	4.95	71.39	0.0	10304260	0.0052	0.51

Table 6
Top 30% TF1 and NF3

	Drifters N= 330			Non-Drifters N= 6,594			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	80.28	193.15	30.5	92.31	269.92	27.0	1037039	0.08	0.52
N. days active	38.75	50.85	20.0	40.78	68.02	17.0	1010601	0.01	0.54
Diversification									
SDI	0.51	0.35	0.6	0.51	0.36	0.6	1075500	0.36	0.51
N. cat.	3.65	2.29	3.0	3.53	2.25	3.0	1054491	0.17	0.52
N. sub-cat	7.26	8.33	5.0	7.22	8.54	4.0	1078888	0.40	0.50
Business									
N. $ sign	2.88	7.64	0.0	3.32	19.89	0.0	1041784	0.08	0.52
Prop. $ sign	0.04	0.09	0.0	0.04	0.08	0.0	1050250	0.12	0.52
Specific Topics									
Search Engine	6.30	21.47	0.0	9.39	38.69	0.0	1077164	0.37	0.50
Monetizing sites	16.84	47.42	1.0	18.16	75.96	1.0	1074137	0.34	0.51
Practical opt.	8.11	19.58	0.0	11.84	57.48	1.0	1076778	0.37	0.51
Comm. of prof.	18.86	90.87	1.0	12.66	74.35	0.0	987551	0.00	0.55
Site building	9.81	27.99	1.0	14.66	83.19	1.0	1083730	0.45	0.50
Exch. and sale	3.25	9.22	0.0	4.26	17.42	0.0	1070570	0.28	0.51
Purch. traffic	1.64	10.14	0.0	1.99	18.25	0.0	1065357	0.18	0.51
Work web master	2.25	8.09	0.0	2.72	10.81	0.0	1048752	0.08	0.52
Not about work	13.22	79.34	0.0	16.65	130.85	0.0	1050045	0.09	0.52

Time Filter 2 (TF2): From 2016 to 2019
Name Filter 1 (NF1): Minimum of five characters in usernames

Table 7
Entire Platform Population TF2 and NF1

	Drifters N= 1,160			Non-Drifters N= 22,188			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	39.65	195.37	4.0	28.72	148.13	4.0	12085308	0.0002	0.53
N. days active	17.78	48.50	3.0	13.41	40.20	2.0	11917918	0.0000	0.54
Diversification									
SDI	0.33	0.40	0.0	0.29	0.39	0.0	12136276	0.0001	0.53
N. cat.	2.14	1.85	1.0	1.97	1.68	1.0	12127189	0.0001	0.53
N. sub-cat	3.65	6.36	1.0	3.14	5.34	1.0	12173247	0.0003	0.53
Business									
N. $ sign	1.71	14.74	0.0	1.02	10.46	0.0	12149912	0.0000	0.53
Prop. $ sign	0.04	0.13	0.0	0.04	0.13	0.0	12191079	0.0000	0.53
Specific Topics									
Search Engine	3.21	19.41	0.0	2.93	21.22	0.0	12838389	0.4260	0.50
Monetizing sites	8.85	92.91	0.0	5.61	36.95	0.0	12794157	0.3434	0.50
Practical opt.	4.16	21.11	0.0	3.80	31.51	0.0	12812234	0.3780	0.50
Comm. of prof.	7.31	54.56	0.0	3.89	40.56	0.0	12113545	0.0000	0.53
Site building	5.24	29.10	0.0	4.60	45.47	0.0	12257289	0.0004	0.52
Exch. and sale	1.69	8.78	0.0	1.45	9.57	0.0	12349774	0.0005	0.52
Purch. traffic	1.14	12.33	0.0	0.65	9.67	0.0	12684530	0.0577	0.51
Work web master	1.02	5.13	0.0	0.96	6.02	0.0	12698689	0.1165	0.51
Not about work	7.03	68.05	0.0	4.83	70.70	0.0	12503083	0.0018	0.51

Table 8
Top 30% TF2 and NF1

	Drifters N=379			Non-Drifters N= 6,545			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	115.09	329.46	33.00	90.39	262.65	27.0	1141394	0.00	0.54
N. days active	49.56	75.52	21.00	40.17	66.76	17.0	1116426	0.00	0.55
Diversification									
SDI	0.52	0.35	0.60	0.51	0.36	0.6	1213995	0.24	0.51
N. cat.	3.75	2.37	3.00	3.53	2.25	3.0	1177444	0.05	0.53
N. sub-cat	8.03	9.68	5.00	7.18	8.45	4.0	1197362	0.13	0.52
Business									
N. $ sign	4.97	25.50	1.00	3.21	19.08	0.0	1124717	0.00	0.55
Prop. $ sign	0.04	0.09	0.01	0.04	0.08	0.0	1149742	0.00	0.54
Specific Topics									
Search Engine	9.35	33.13	0.00	9.23	38.32	0.0	1216732	0.25	0.51
Monetizing sites	26.00	161.32	1.00	17.63	66.48	1.0	1207479	0.18	0.51
Practical opt.	11.93	35.69	1.00	11.65	57.22	1.0	1204423	0.16	0.51
Comm. of prof.	21.47	93.95	0.00	12.46	73.97	0.0	1132597	0.00	0.54
Site building	14.83	49.56	1.00	14.40	82.89	1.0	1180834	0.05	0.52
Exch. and sale	4.38	14.93	0.00	4.20	17.24	0.0	1206242	0.15	0.51
Purch. traffic	3.17	21.43	0.00	1.90	17.72	0.0	1220897	0.23	0.51
Work web master	2.60	8.69	0.00	2.71	10.80	0.0	1239948	0.50	0.50
Not about work	21.36	117.87	0.00	16.20	129.47	0.0	1157260	0.00	0.53

Time Filter 2 (TF2): From 2016 to 2019
Name Filter 2 (NF2): Minimum of six characters in usernames

Table 9
Entire Platform Population TF2 and NF2

	Drifters N= 924			Non-Drifters N= 22,424			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	33.64	184.53	4.0	29.08	149.29	4.0	9987036	0.03	0.52
N. days active	16.23	46.29	3.0	13.52	40.41	2.5	9861071	0.01	0.52
Diversification									
SDI	0.32	0.40	0.0	0.29	0.39	0.0	9880754	0.00	0.52
N. cat.	2.10	1.82	1.0	1.97	1.68	1.0	9927170	0.01	0.52
N. sub-cat	3.49	6.18	1.0	3.16	5.36	1.0	10056632	0.05	0.51
Business									
N. $ sign	1.63	15.80	0.0	1.03	10.45	0.0	9899181	0.00	0.52
Prop. $ sign	0.04	0.13	0.0	0.04	0.13	0.0	9922078	0.00	0.52
Specific Topics									
Search Engine	2.65	13.88	0.0	2.95	21.38	0.0	10208775	0.15	0.51
Monetizing sites	8.80	101.76	0.0	5.65	37.03	0.0	10359620	0.50	0.50
Practical opt.	3.80	20.97	0.0	3.82	31.42	0.0	10227283	0.21	0.51
Comm. of prof.	5.06	34.42	0.0	4.02	41.64	0.0	9914873	0.00	0.52
Site building	4.90	29.07	0.0	4.62	45.33	0.0	9994147	0.01	0.52
Exch. and sale	1.85	9.67	0.0	1.44	9.52	0.0	9928202	0.00	0.52
Purch. traffic	0.84	8.24	0.0	0.67	9.88	0.0	10172462	0.04	0.51
Work web master	1.11	5.54	0.0	0.96	5.99	0.0	10120283	0.03	0.51
Not about work	4.62	55.54	0.0	4.96	71.12	0.0	10200365	0.08	0.51

Table 10
Top 30% TF2 and NF2

	Drifters N= 290			Non-Drifters N= 6,634			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	100.70	319.63	32.50	91.35	264.24	27.0	901275.5	0.03	0.53
N. days active	46.66	74.06	21.00	40.42	66.98	17.0	883153.0	0.01	0.54
Diversification									
SDI	0.51	0.35	0.60	0.51	0.36	0.6	953309.5	0.40	0.50
N. cat.	3.72	2.38	3.00	3.53	2.25	3.0	923191.0	0.12	0.52
N. sub-cat	7.83	9.61	4.00	7.20	8.48	4.0	954144.0	0.41	0.50
Business									
N. $ sign	4.91	27.95	1.00	3.23	19.03	0.0	874416.5	0.00	0.55
Prop. $ sign	0.04	0.09	0.01	0.04	0.08	0.0	883824.0	0.01	0.54
Specific Topics									
Search Engine	7.93	23.93	0.00	9.30	38.55	0.0	961451.0	0.49	0.50
Monetizing sites	26.89	180.52	1.00	17.71	66.51	1.0	946161.0	0.31	0.51
Practical opt.	11.31	36.34	1.00	11.68	56.97	1.0	947644.0	0.32	0.51
Comm. of prof.	15.32	60.22	0.00	12.85	75.81	0.0	889351.5	0.01	0.54
Site building	14.36	50.64	1.00	14.43	82.50	1.0	927042.5	0.13	0.52
Exch. and sale	5.04	16.75	0.00	4.18	17.14	0.0	921030.0	0.07	0.52
Purch. traffic	2.30	14.58	0.00	1.96	18.08	0.0	947265.5	0.26	0.51
Work web master	2.95	9.55	0.00	2.69	10.75	0.0	937842.0	0.18	0.51
Not about work	14.60	98.53	0.00	16.56	130.03	0.0	921150.0	0.07	0.52

Time Filter 3 (TF2) : From 2017 and 2018
Name Filter 1 (NF2): Minimum of five characters in usernames

Table 11
Entire Platform Population TF3 and NF1

	Drifters N=696			Non-Drifters N= 22,652			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	36.09	196.98	4.0	29.05	149.19	4.0	7396325	0.00	0.53
N. days active	17.37	47.53	3.0	13.51	40.43	2.5	7317611	0.00	0.54
Diversification									
SDI	0.33	0.40	0.0	0.29	0.39	0.0	7405017	0.00	0.53
N. cat.	2.16	1.85	1.0	1.97	1.68	1.0	7409644	0.00	0.53
N. sub-cat	3.63	6.41	1.0	3.16	5.36	1.0	7442372	0.00	0.53
Business									
N. $ sign	1.90	18.41	0.0	1.03	10.39	0.0	7421517	0.00	0.53
Prop. $ sign	0.04	0.13	0.0	0.04	0.13	0.0	7442708	0.00	0.53
Specific Topics									
Search Engine	2.92	16.13	0.0	2.94	21.27	0.0	7871826	0.47	0.50
Monetizing sites	11.05	118.45	0.0	5.61	36.72	0.0	7832678	0.36	0.50
Practical opt.	3.48	15.49	0.0	3.83	31.43	0.0	7879421	0.49	0.50
Comm. of prof.	5.57	29.44	0.0	4.02	41.69	0.0	7371457	0.00	0.53
Site building	3.98	19.01	0.0	4.65	45.36	0.0	7535437	0.01	0.52
Exch. and sale	2.00	10.64	0.0	1.44	9.49	0.0	7526997	0.00	0.52
Purch. traffic	1.39	14.40	0.0	0.65	9.65	0.0	7633722	0.00	0.52
Work web master	1.21	5.93	0.0	0.96	5.98	0.0	7758455	0.13	0.51
Not about work	4.48	50.46	0.0	4.96	71.10	0.0	7728462	0.06	0.51

Table 12
Top 30% TF3 and NF1

	Drifters N=231			Non-Drifters N=6,693			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	102.62	332.54	31.00	91.37	264.23	27.0	728492	0.07	0.53
N. days active	47.66	73.76	21.00	40.44	67.06	17.0	707074	0.01	0.54
Diversification									
SDI	0.52	0.35	0.63	0.51	0.36	0.6	756048	0.28	0.51
N. cat.	3.74	2.37	3.00	3.53	2.25	3.0	736946	0.11	0.52
N. sub-cat	7.84	9.78	5.00	7.20	8.48	4.0	758913	0.32	0.51
Business									
N. $ sign	5.48	31.70	1.00	3.23	18.92	0.0	695031	0.00	0.55
Prop. $ sign	0.05	0.09	0.01	0.04	0.08	0.0	697116	0.00	0.55
Specific Topics									
Search Engine	8.35	27.22	0.00	9.27	38.37	0.0	770912	0.47	0.50
Monetizing sites	32.34	204.24	1.00	17.60	65.99	1.0	760147	0.32	0.51
Practical opt.	9.77	25.77	1.00	11.73	57.02	1.0	754084	0.25	0.51
Comm. of prof.	15.84	49.57	0.00	12.85	75.95	0.0	717639	0.02	0.54
Site building	10.90	31.88	1.00	14.55	82.60	1.0	744830	0.16	0.52
Exch. and sale	5.18	17.99	0.00	4.18	17.09	0.0	747174	0.15	0.52
Purch. traffic	3.76	24.83	0.00	1.91	17.66	0.0	753183	0.17	0.51
Work web master	3.15	9.95	0.00	2.69	10.72	0.0	751674	0.18	0.51
Not about work	13.33	87.04	0.00	16.59	130.07	0.0	746690	0.14	0.52

Time Filter 3 (TF3): From 2017 and 2018
Name Filter 2 (NF2): Minimum of six characters in usernames

Table 13
Entire Platform Population TF3 and NF2

	Drifters N=557			Non-Drifters N= 22,791			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	33.39	212.15	4.0	29.16	149.03	4.0	6112769	0.07	0.52
N. days active	15.99	46.98	3.0	13.57	40.50	3.0	6048591	0.03	0.52
Diversification									
SDI	0.33	0.41	0.0	0.29	0.39	0.0	5958426	0.00	0.53
N. cat.	2.15	1.84	1.0	1.97	1.68	1.0	5991509	0.00	0.53
N. sub-cat	3.54	6.37	1.0	3.16	5.37	1.0	6112788	0.05	0.52
Business									
N. $ sign	1.87	19.92	0.0	1.03	10.39	0.0	6071896	0.01	0.52
Prop. $ sign	0.04	0.13	0.0	0.04	0.13	0.0	6088850	0.01	0.52
Specific Topics									
Search Engine	2.52	12.78	0.0	2.95	21.30	0.0	6287850	0.30	0.50
Monetizing sites	10.90	129.54	0.0	5.65	36.86	0.0	6253243	0.24	0.51
Practical opt.	3.31	15.52	0.0	3.83	31.36	0.0	6323919	0.43	0.50
Comm. of prof.	4.51	24.30	0.0	4.05	41.70	0.0	5965911	0.00	0.53
Site building	3.48	16.60	0.0	4.66	45.27	0.0	6130521	0.05	0.52
Exch. and sale	2.24	11.71	0.0	1.44	9.47	0.0	5989857	0.00	0.53
Purch. traffic	1.14	10.42	0.0	0.66	9.81	0.0	6100427	0.00	0.52
Work web master	1.34	6.47	0.0	0.95	5.96	0.0	6177571	0.05	0.51
Not about work	3.96	54.07	0.0	4.97	70.93	0.0	6330213	0.42	0.50

Table 14
Top 30% TF3 and NF2

	Drifters N= 177			Non-Drifters N=6,747			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	98.68	368.63	31.00	91.56	263.60	27.0	569759	0.15	0.52
N. days active	45.41	75.44	20.00	40.56	67.07	17.0	552251	0.04	0.54
Diversification									
SDI	0.52	0.35	0.64	0.51	0.36	0.6	580491	0.26	0.51
N. cat.	3.79	2.38	3.00	3.53	2.25	3.0	562096	0.09	0.53
N. sub-cat	7.81	9.97	5.00	7.21	8.49	4.0	595128	0.47	0.50
Business									
N. $ sign	5.62	35.10	1.00	3.24	18.90	0.0	540025	0.01	0.55
Prop. $ sign	0.05	0.10	0.01	0.04	0.08	0.0	536585	0.01	0.55
Specific Topics									
Search Engine	7.45	21.87	0.00	9.29	38.39	0.0	595110	0.47	0.50
Monetizing sites	33.38	228.61	1.00	17.69	66.18	1.0	583177	0.29	0.51
Practical opt.	9.67	26.46	1.00	11.72	56.83	1.0	587471	0.35	0.51
Comm. of prof.	13.32	41.81	1.00	12.94	75.90	0.0	539074	0.01	0.55
Site building	9.78	28.44	1.00	14.55	82.35	1.0	589704	0.38	0.51
Exch. and sale	6.07	20.19	0.00	4.16	17.04	0.0	556765	0.04	0.53
Purch. traffic	3.06	18.33	0.00	1.94	17.94	0.0	579546	0.17	0.51
Work web master	3.65	11.08	0.00	2.68	10.69	0.0	562733	0.05	0.53
Not about work	12.29	95.56	0.00	16.59	129.63	0.0	593886	0.44	0.50

Time Filter 3 (TF3): From 2017 and 2018
Name Filter 3 (NF3): Minimum of five characters AND at least an uppercase OR a number OR one special character in usernames

Table 15
Entire Platform TF3 and NF3

	Drifters N=421			Non-Drifters N= 22,927			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	28.53	75.86	4.0	29.27	151.87	4.0	4404273	0.00	0.54
N. days active	16.34	36.23	3.0	13.58	40.74	3.0	4356994	0.00	0.55
Diversification									
SDI	0.33	0.40	0.0	0.29	0.39	0.0	4524930	0.01	0.53
N. cat.	2.19	1.86	1.0	1.97	1.68	1.0	4479288	0.00	0.54
N. sub-cat	3.54	5.77	1.0	3.16	5.39	1.0	4534297	0.01	0.53
Business									
N. $ sign	1.13	4.93	0.0	1.05	10.79	0.0	4483080	0.00	0.54
Prop. $ sign	0.04	0.13	0.0	0.04	0.13	0.0	4510193	0.00	0.53
Specific Topics									
Search Engine	2.62	16.15	0.0	2.95	21.22	0.0	4796942	0.39	0.50
Monetizing sites	8.79	40.19	0.0	5.72	41.58	0.0	4718437	0.17	0.51
Practical opt.	2.53	8.94	0.0	3.84	31.33	0.0	4656851	0.07	0.52
Comm. of prof.	5.46	29.91	0.0	4.04	41.56	0.0	4401129	0.00	0.54
Site building	2.73	9.38	0.0	4.66	45.19	0.0	4577963	0.01	0.53
Exch. and sale	1.60	6.71	0.0	1.46	9.57	0.0	4550360	0.00	0.53
Purch. traffic	0.56	2.25	0.0	0.68	9.91	0.0	4655954	0.01	0.52
Work web master	1.26	6.37	0.0	0.96	5.97	0.0	4802565	0.39	0.50
Not about work	2.97	19.70	0.0	4.98	71.17	0.0	4717719	0.08	0.51

Table 16
Top 30% TF3 and NF3

	Drifters N=152			Non-Drifters N= 6,772			Statistics		
	Mean	std	Median	Mean	std	Median	Mannwhitneyu	p-value	1-f
Activity Rate									
N. posts	73.76	113.04	31.50	92.14	269.20	27.0	486970	0.13	0.53
N. days active	41.24	51.68	21.00	40.67	67.61	17.0	467977	0.03	0.55
Diversification									
SDI	0.51	0.35	0.60	0.51	0.36	0.6	512991	0.47	0.50
N. cat.	3.71	2.31	3.00	3.54	2.25	3.0	492061	0.17	0.52
N. sub-cat	7.18	8.39	5.00	7.23	8.53	4.0	511404	0.45	0.50
Business									
N. $ sign	2.89	7.89	1.00	3.31	19.67	0.0	461471	0.01	0.55
Prop. $ sign	0.05	0.10	0.02	0.04	0.08	0.0	459530	0.01	0.55
Specific Topics									
Search Engine	6.95	26.37	0.00	9.29	38.28	0.0	503464	0.31	0.51
Monetizing sites	23.54	64.40	2.00	17.97	75.06	1.0	478807	0.06	0.53
Practical opt.	6.53	14.00	0.00	11.78	56.84	1.0	495430	0.20	0.52
Comm. of prof.	14.28	48.62	1.00	12.92	75.71	0.0	467051	0.02	0.55
Site building	6.59	14.79	1.00	14.60	82.29	1.0	513136	0.47	0.50
Exch. and sale	3.53	10.78	0.00	4.23	17.24	0.0	514151	0.49	0.50
Purch. traffic	1.18	3.48	0.00	1.99	18.14	0.0	505982	0.30	0.51
Work web master	3.05	10.30	0.00	2.69	10.71	0.0	512595	0.46	0.50
Not about work	8.10	32.21	0.00	16.67	130.21	0.0	501689	0.26	0.51