Cybercrime: The Industry of Anonymity

Jonathan Lusthaus
Department of Sociology



Thesis submitted for the degree of Doctor of Philosophy
University of Oxford

2016

Abstract

The central theme of this thesis is that cybercrime has matured into a large profit-driven industry. Hobby hackers still exist and hacktivists have attracted some attention in recent years, but a very significant component of contemporary cybercrime is now financially motivated. While its goods and services are usually illicit, the cybercrime industry operates according to the same broad principles of industrial organisation observed across numerous other contexts. But the development of this industry is somewhat puzzling. Ostensibly much cybercriminal cooperation takes place online. As a result, cybercriminals are often partnering with online criminals whose true identities are unknown to them. They also have no means of physical enforcement should deals go awry. Partnering with conventional criminals, who operate outside the protection of the state, already appears to present significant challenges for cooperation. The challenge of anonymity makes cooperation even more difficult and suggests that cybercriminals would often act alone, or in small groups. Instead a large successful industry has formed. This thesis first addresses the industrialisation of cybercrime. It then addresses this puzzle of how cybercriminals have overcome the challenges to cooperation to build an industry on such a scale.

Acknowledgements

This thesis would not have been possible without the participation of over 200 subjects. I began my work on cybercrime in 2011 with no knowledge at all of the topic. From the beginning, participants generously shared their time and wisdom with me. In short, they educated me. Some went further and took it upon themselves to champion this study: to open their networks and recommend other potential interview subjects; to send me relevant sources to read; and to take me under their protection and help me feel welcome (and safe) in foreign countries. As much as I have weaved this study together from a range of different sources, at a foundational level it encapsulates the experiences, knowledge and insights of these subjects. This thesis is as much theirs as it is mine. Due to the restrictions of maintaining their anonymity, I cannot acknowledge them by name. But I owe them the greatest thanks.

I also benefitted greatly from the help of many others who were not formal participants of this study. Many were friends already, while others I encountered along the journey and they simply wished to help. All showed me great kindness. Some made introductions to potential subjects; others gave me travel and safety tips. Some met me for meals or let me sleep on their couches! I can't name everyone who helped me along the way for the fear that I would almost certainly forget someone (it would also extend these acknowledgements by many pages). Additionally, it does not seem appropriate to thank this category by name, while those above remain anonymous. But, again, my gratitude to all those who helped me is deep.

This was a very costly study to undertake, because it involved so much travel. I was forced to carry out many of the trips in a very miserly fashion, often undertaking research when I had other reasons for passing through a country. There were certain field visits that would not have been possible without the generous support of others. Nuffield College provided a generous research allowance each year, which contributed to a number of the trips. The college also provided two travel fund grants that specifically allowed me to visit China and Nigeria. One could not ask for a better-resourced, more supportive academic environment to work in. I was also the beneficiary of a John Fell Fund grant, alongside Professor Federico Varese, which allowed a second visit to Romania. Finally, the Commonwealth Bank of Australia generously provided a no-strings-attached donation to cover research costs towards the end of the project. This ensured that I had the funding to visit some essential locations that remained on my list of hotspots, most notably Ukraine. I thank the bank for their uncharacteristic vision and for understanding the value of independent academic research.

In academic terms, I wish to thank all those who read part or all of this thesis at various points. Heather Hamill and Paolo Campana acted as examiners for my Transfer of Status. David Kirk and Lucas Kello served the same role in my Confirmation of Status. The points of support and challenge in these meetings were equally valuable in clarifying my thinking and enhancing this project. David Dixon, Laurin Weissinger, Paolo Campana and Jamie Collier all read one or more chapters of this thesis, while Michael Hart read a near complete version of the manuscript. I thank them all for spending the time and providing very useful comments. Ben Taaffe

provided speedy and thorough comments on the copy. While not reading the thesis, conversations with Ask Neve helped me clarify important aspects of the theoretical background I have used.

I express enormous gratitude to my supervisor, Professor Federico Varese. I could not have hoped for a better supervisor. He has been a constant source of encouragement and support. From the beginning he has helped in framing the project. I benefitted greatly from his incisive mind, particularly his ability to see each project on it's own terms, rather than offering a cookie-cutter view of how good research must be done. While the writing and ideas contained herein are all my own, the intellectual parentage is clear. I also wish to thank Valeria Pizzini-Gambetta who supervised my masters thesis, which was the origin of this project and still remains strongly connected to this final product. My doctorate was undertaken as a Clarendon Scholar. My studies would not have been possible without the joint support of the Clarendon Fund and Nuffield College.

I wish to thank my partner. She has been my companion throughout the journey, both metaphorically and literally. Her patient agreement to largely spend our holidays in cybercrime hotspots has played a huge role in allowing this study to be completed. Through this process, she has become somewhat of an expert on cybercrime herself! She has been a constant source of support and someone to bounce ideas off. She assisted me greatly in the final stages of the doctorate, ensuring that everything came together in time.

I would also like to thank my whole family, whose love and support travels with me wherever I go. In particular, I dedicate this book to my parents. My father had dreams of being a political economist, but life went another way. He had a fascination with China and Russia and it is perhaps fitting that my study of cybercrime lead me both to economic sociology and an opportunity to study such countries. I hope very much that he would have enjoyed reading this thesis. My mother has fought for me my entire life and has constantly challenged me to pursue big ideas. This thesis is a testament to how she has raised me, and I hope lives up to the model that she has set me from a young age.

Table of Contents

List of Tables/Figures **2**

1. Introduction **1**
Industry of Anonymity 3
What is Cybercrime? 8
Who are the Cybercriminals? 14
Literature Review and Theoretical Background 21
Literature Review 23
Theory 27
Approach and Structure 37

2. Data and Methods **39**
Research Style 39
Data Sources 44
Scope, Sampling and Limitations 49
Geographical Sampling 51
Purposive Sampling 55
Snowball Sampling 65
Accuracy and Limitations 67
Ethics 75
Inmates and Ethics 80
Incriminating Admissions 81
Informed Consent and Potential Coercion 83
Weakened Anonymity and Confidentiality 85
Conclusion 86

3. The Evolution of Profit-Driven Cybercrime: From Lone Wolves to Industrialisation 87
A Brief History of Hacking 89
The Turn to Profit 92
The Golden Age of Forums 95
The Specialisation and Fragmentation of the Market 106
The Development of Operational Structures 114
The Growth of Cybercriminal "Infrastructure" 116
The Current State of Cybercrime and Cybercriminals 119
Conclusion 122

4. Making Sense of the Cybercrime Industry **124**
Specialisation 124
Professionalisation 134
Markets 140
Firms 145
Conclusion 150

5. Nicknames and Identity **152**
Nicknames as Brands 156
Choosing Nicknames 160
Interpreting Nicknames 164
Balancing Anonymity with Identity 168
Conclusion 176

6. How Cybercriminals Cooperate Online **178**
Trustworthiness 179
Reputation 179
Appearance 190
Performance 197
Enforcement 203
Risk for Reward? 214
Failures of Cooperation 218
Conclusion 220

7. The Offline Dimension **223**
Offline Interactions 224
Why Offline? 235
Failures of Cooperation 246
A Balance Between Online and Offline? 248
Conclusion 251

8. Cybercrime, Organised Crime and Governance **253**
Cybercrime and Organised Crime 255
Corruption and Protection 266
Corruption and Protection in the Former Soviet Bloc 270
Conclusion 275

9. Conclusion **277**

Bibliography **289**

Appendix: List of Participants **300**

List of Tables

1. Profession Codes **78**

2. Country Codes **78**

3. Types of Aliases **153**

List of Figures

1. Online Card Shop **139**

2. Referee Post **184**

3. Forum Menu Page with “Scammers” Section **188**

4. Joining Date **196**

5. Prowess Demonstration Post **197**

6. Private Message Reply 1 **198**

7. Private Message Reply 2 **198**

8. Verified Vendor Requirement **200**

1. Introduction

On July 5, 2014 a thirty-year-old Russian national from Vladivostok named Roman Seleznev was reaching the end of his holiday. He had been in the Maldives with his girlfriend and daughter. At the conclusion of the trip, they boarded a seaplane to travel from their five star resort to Malé's international airport. As a bus ferried them from the seaplane to the terminal, Seleznev may not have noticed but he was being watched closely from the rows behind him. When he arrived at the airport, his passport was checked and he began a long journey. But the destination was not the one he had planned. He was on his way to the U.S. territory of Guam, and he began his travel in handcuffs (Wilber and Strohm 2015).

When one looks at published photos of Seleznev and his family, their appearance is remarkably normal. Seleznev cuts a casual and jovial figure, who could easily pass for a family minded IT professional or technology entrepreneur. In a sense, this may be an accurate descriptor. But other published photos indicate something more. One shows Seleznev next to a bright yellow Dodge muscle car, parked in Red Square in Moscow. Others show bundles of cash in the back seat of a vehicle or him partying with friends. These pictures are more suggestive of someone with a taste for the high life and whose earnings may be less than legitimate. But taken together these divergent images of Seleznev are perhaps fitting for someone who is alleged to be one of the leading cybercriminals of recent years (for published photos see RT 2014, Carter 2015, Pulkkinen 2015).

According to a U.S. indictment, Seleznev was engaged in credit card fraud on a massive scale. His common tactic was to infect the point of sale systems and computers of retail businesses, such as restaurants, with malware. Once these were infected, Seleznev and his associates could gain access to the credit card details of myriad customers. While he likely had other periods of activity, the indictment alleges that between November 15, 2010 and February 22, 2011 Seleznev and his associates stole over 200,000 credit card numbers. Through his online shopping websites, he sold around 140,000 card numbers to other cybercriminals, which generated at least US$2,000,000 in profits.[1] He would also have made considerable income from the cards he kept for the use of himself and his associates. Prosecutors suggested that Seleznev's team had earned at least around US$18,000,000 from his activities (Carter 2015). An earlier indictment in 2012, listed Seleznev as a member of the "Carder.su organization". This forum provided a thriving online marketplace where credit card data among other illicit goods and services could be traded between cybercriminals from around the world. Seleznev would advertise his wares like any good merchant. The forum as a whole was claimed to be responsible for more than US$50,000,000 in fraudulent charges.[2]

Given this background, it's perhaps not surprising that Seleznev was apprehended in the Maldives. He might have arrived as a family man, but he left as a cybercriminal. While he chose to holiday in that country as it did not have an extradition treaty with America, U.S. Secret Service agents managed to negotiate an ad hoc arrangement with the local authorities. Once Seleznev was handed over to the Secret Service, he

[1] *US v. Roman Seleznev and Others*, United States District Court, Western District of Washington, 2011 [indictment].
[2] *US v. Roman Zolotarev and Others*, United States District Court, Nevada, 2012 [indictment].

was flown to Guam where he was charged under U.S. law. Following this, he was later transferred to Seattle to face trial and, at the time of writing, is awaiting sentence (Wilber and Strohm 2015).

Industry of Anonymity

For a number of reasons, this story makes for an appropriate opening to a thesis on the sociology of cybercrime, but central among these is to put a human face on the subject. There can be a temptation to view cybercrime as an almost invisible phenomenon. Attacks occur through cyberspace and are orchestrated by unseen and unknown actors. We only have a picture of the victim in each case. This leads to a mystification of cybercrime and a focus on the technical components rather than the offenders, which makes the phenomenon even more foreign to the average person. The reality, of course, is somewhat different. As the example of Roman Seleznev shows, every attack has one or more humans behind it. Somewhere in the world, there is always a person sitting at a keyboard. That person has a life and exists in a specific social setting. Both the people behind cybercrime and the contexts in which they operate deserve significant scholarly attention. It is hoped that this thesis can, in part, help lift the veil of anonymity that has hidden cybercrime offenders and their activities from view.

Seleznev's story is important for another major reason: his tale is reflective of broader shifts in the world of cybercrime. The picture painted above is of a multi-millionaire criminal tech entrepreneur who, with his associates, is capable of compromising a large number of businesses and siphoning off hundreds of thousands of card details.

Seleznev not only exploits these cards himself, but also takes his wares to market. He advertises them on a marketplace with thousands of members and sells through automated online shopfronts, netting millions of dollars in the process. This is a far cry from earlier days of cybercrime and the residual image of the teenager in his mother's basement that still occupies a place in the zeitgeist. It also illustrates the long development that has taken place from the early days of mainframe computer hacking in the late 1950s, which was an ostensibly legal activity largely driven by intellectual curiosity.

The central theme of this thesis is that cybercrime has matured into a large profit-driven industry. Hobby hackers still exist and hacktivists have attracted some attention in recent years, but a very significant component of contemporary cybercrime is now financially motivated. Contemporary cybercriminal enterprises encompass, among other activities, blackmail, extortion, intellectual property violations, phishing, fraud, identity theft, spam, and renting out resources and services (such as hacking services). This facet of cybercrime is organised, sophisticated and on a large scale. Although there are significant methodological and data challenges to this, government and private sector studies regularly estimate that global cybercrime could cost hundreds of billions of dollars a year.[3] A study by the United Nations claimed that the victimization levels of conventional crime might now be falling behind those of cybercrime (UNODC 2013, p. 28).

[3] For a survey of different estimates see Morgan (2016). But these figures should be viewed with caution. This is a controversial area with a number of loose claims, limited data and certain agendas that may benefit from hyping the threat. While the problem is no doubt large, some scholars have pushed back and advocated for a more measured approach in estimating the costs of cybercrime (Anderson et al. 2013).

But the conception of cybercrime as an industry is more about the way it functions, rather than the significant amounts of money it generates its proponents and costs its victims. While one can become trapped in a definitional quagmire, in simple terms an industry consists of businesses that operate in similar ways and produce the same types of goods and services (see Nightingale 1978). While its goods and services are usually illicit, the cybercrime industry operates according to the same broad principles of industrial organisation observed across numerous other contexts (see Church and Ware 2000, Hay and Morris 1979). First, there is a clear division of labour, with a number of cybercriminal specialties from hacking, to coding, to vending, to "cashing out" - which involves turning virtual gains into monetary or physical ones. In fact, there are numerous subspecialties within these specialties. As a result, there is now a wide range of people involved in cybercrime, with offenders representing many ages, demographic groups, skillsets and backgrounds. The threat is no longer just lone hackers operating for recreation, but includes much more professional criminals, who are driven by financial motivations rather than the old hacker code of intellectual discovery and information sharing. Overall, alongside specialisation there has been a strong professionalisation of cybercrime.

Second, the increasing specialisation of cybercriminals is mirrored by the growth of online markets. In this regard, virtual marketplaces, which somewhat resemble criminal eBays, have become particularly important. On each of these forums, up to thousands of cybercriminals can meet and trade illicit goods and services online. Common products that are traded include compromised credit and debit card data, online banking logins and malware, as well as services like cashing out schemes. Finally, cybercriminals increasingly operate in groups, which begin somewhat to

resemble “firms” (businesses). Many of these are small crew-like groups with members carrying out particular roles. They could produce malware as a team or carry out elaborate confidence scams online. As we shall see, at their furthest point of sophistication some of these firms are almost indistinguishable from licit companies, with physical office space and corporate hierarchies. These could be companies that specialise in coordinating spam advertising campaigns or serve as bulletproof hosts, which are essentially internet service providers that refuse to take down illegal content.

While an industry of profit-driven cybercrime has undoubtedly arisen, its development is somewhat puzzling. Ostensibly much cybercriminal cooperation takes place online. As a result, cybercriminals are often partnering with online criminals whose true identities are unknown to them. They also have no means of physical enforcement should deals go awry. Partnering with conventional criminals already appears to present significant challenges for cooperation: criminals operate outside the law and the protection of the state, so they must work somewhat secretly in a world of distrust. Campana and Varese (2013, p. 265) summarise the increased challenges facing criminals in this way:

> In the underworld, actors face more natural obstacles to be overcome. By definition, one cannot turn to the state to protect stolen or illegal assets. Information about the quality of goods and services is hard to come by, as there are no reputable and easily accessible sources of unbiased information. One cannot even be sure that the person offering a deal is not an undercover agent or a police informant. Regardless of personal inclination to cheat, actors in the underworld are difficult to locate, as they move around frequently. Entrepreneurs in these markets cannot freely advertise their good reputation, creditors disappear, informants consort with the police, and undercover agents try to pass themselves off as *bona fide* fellow criminals”.

In response to such apparent challenges, a relatively significant body of literature has emerged examining how trust can be buttressed in a number of criminal (among other extra-legal) settings, leading to successful cooperation where it would naturally seem unlikely (Gambetta 1993, 2009a, Varese 2001, Campana and Varese 2013, Skarbek 2011, Levi 2008, Reuter 1983).

But cybercrime takes these complications one step further by introducing the element of anonymity. This creates further challenges in addition to those facing conventional criminals. It is true that some conventional criminals may try to protect their identities to the point of being nearly anonymous, but this is nowhere near the scale of anonymous activity that defines cybercrime. In such an environment, it is difficult to assess trustworthiness and enforce agreements when you don't even have physical interactions to indicate with whom you are dealing. This is not to mention that if you did manage to identify your collaborators, they might be dispersed around the globe. This type of setting appears to offer little hope for physical violence, which has often been a pillar of enforcing cooperation among traditional criminals.

As a result of these "extreme" challenges, it might be expected that cybercriminals would often act alone and not in collaboration. Nonetheless, in recent years cybercriminals have increasingly formed links with other criminals. There is a now a fully-fledged cybercrime industry, with clear elements not only of low-level collaboration, but also facets of broader organisation and governance (Lusthaus 2012, 2013b, Holt and Lampke 2010, Kshetri 2010). The focus of this thesis is twofold. First, it seeks to outline the development of the cybercrime industry and how it functions. Second, it addresses the puzzle of how this industry has developed when

facing the challenges of anonymity. Anonymity lies at the heart of making sense of cybercrime. First we must peel back some layers of anonymity to be able to understand how cybercrime works, rather than view it as a mystical and invisible phenomenon. Then we must understand how cybercriminals seek to overcome the challenges of dealing with anonymous partners in order to build a functioning industry. Finally, we also need to acknowledge those instances where cybercriminals choose not to embrace anonymity and may seek to operate with physically known partners instead. This too may have a significant impact on the successful functioning of the broader cybercrime industry.

Before proceeding with the discussion of cybercriminal industrialisation and anonymity, it is important to outline some preliminary matters. The rest of this introduction: 1) settles on an appropriate definition of cybercrime; 2) provides background on the nature of cybercriminal offenders; 3) surveys the relevant literature on the topic of profit-driven cybercrime and key theoretical background; 4) outlines the approach and structure of the thesis.

What is Cybercrime?

Many of the early investigations of cybercrime struggled with the limited data available at the time and with a subject matter that was rapidly evolving as new technologies emerged. This literature was not necessarily theoretical, but largely attempted to make sense of what this new phenomenon of cybercrime meant in relation to traditional approaches to the study of crime. It outlined key aspects of what cybercrime was, the technologies being used and the new threats posed as the Internet

came into existence and more and more aspects of human life started to go online, including credit card use and banking (Grabosky 2001, Brenner 2002, Yar 2013, Wall 2007, 2001a). The focus of such works was often on cybercrime in general rather than on a specific sub-genus like profit-driven cybercrime. Given how far the Internet and associated technologies have now come, it is interesting to look back on this literature as capturing some of the spirit of the time. It was certainly prescient in a number of ways, but in some other regards, new technologies clearly evolved in ways authors could not have predicted and set cybercrime on a another course.

One of the key contributions made by this conceptual literature on cybercrime has been in attempting to define the term *cybercrime* itself. In the realm of new technologies and crime, there have been a number of competing terms looking at similar, but perhaps distinct, phenomena. These have included: *cybercrime*, *virtual crime*, *net-crime*, *hi-tech crime* and *computer crime*. But, as Wall argues, whatever "its merits and demerits, the term 'cybercrime' has entered the public parlance and we are more or less stuck with it" (Wall 2008, p. 20). In recent years, *cybercrime* appears to have become the dominant term used by social scientists working in this area.

The main conceptual debate around demarcating what is (and is not) cybercrime has been whether cybercrime constitutes a new frontier of crime, or is instead a form of existing criminality in a novel online environment. Some have argued for the former position. For instance, Wall (1998) nodded in this direction by arguing that "the Internet, and particularly the cyberspace it creates, is not just a case of 'old wine in new bottles', or for that matter 'new wine in new bottles', rather many of its characteristics are so novel that the expression 'new wine, but no bottles!' becomes a

more fitting description" (pp. 201-202). On the other hand, many hold for the other (wine-related) approach perhaps best stated by Peter Grabosky in his article "Virtual Criminality: Old Wine in New Bottles?", who suggested that:

> '[V]irtual criminality' is basically the same as the terrestrial crime with which we are familiar. To be sure, some of the manifestations are new. But a great deal of crime committed with or against computers differs only in terms of the medium. While the technology of implementation, and particularly its efficiency, may be without precedent, the crime is fundamentally familiar. It is less a question of something completely different than a recognizable crime committed in a completely different way" (Grabosky 2001, p. 243).

In line with this approach, a consensus has formed around defining cybercrime not as a particular subset of crimes, but rather as a range of illegal activities taking place within the realm of cyberspace (Yar 2005, p. 407). As Holt and Bossler note in their review of the literature in the field, while there is "no single, agreed-on definition of cybercrime, many scholars argue that it involves the use of cyberspace or computer technology to facilitate acts of crime and deviance" (Holt and Bossler 2014, p. 21).

But there is one further element linked to this debate that somewhat muddies the definitional waters. This is the distinction some scholars and practitioners continue to draw between those cybercrimes that are "traditional" crimes facilitated and enhanced by new technologies (*cyber-enabled* or *assisted* crimes such as fraud or theft) and those cybercrimes that could not exist without these new technologies because computers or networks are usually the target (*cyber-dependent* or *focussed* crimes - such as computer/network intrusion, DDoS[4] attacks and the spread of malware).[5] In

[4] Distributed denial of service.

my interactions with law enforcement agencies and policymakers, it is clear that this categorisation has been quite widely adopted.

While there is a distinction to be made here, for application in the social sciences this division seems somewhat illusory. At their heart, crimes are behaviours that have been criminalised by various legal systems: they do not necessarily have an independent theoretical underpinning. Laws might make specific acts against computers and networks criminal, but it has often been the use of new tools that has been criminalised rather than the behaviours behind them. The older motivations remain. For instance, computer intrusions and the spread of malware can facilitate theft or vandalism, while DDoS attacks might be part of an extortion ring or be in support of a political agenda. It would be unusual for one of these technical crimes not to be linked to some broader motivation and a more traditional crime type (theft, fraud, extortion, harassment, vandalism, espionage). For legal studies of cybercrime, this distinction might be relevant, but for social science based approaches, it does not appear particularly helpful. For these latter studies, in terms of understanding the human actors involved in cybercrime, the motivation behind the crimes should probably matter more than legal technicalities.

If there is indeed a sociological distinction between these forms of cybercrime, this study includes both types under the single banner of cybercrime. In this thesis, I apply a broad functional definition: cybercrime as the "use of computers or other electronic devices via information systems such as organisational networks or the Internet to facilitate illegal behaviours" (McQuade 2006, p. 16). It is also sensible to specify that

[5] See, for example, Furnell (2002, p. 22).

the use of such technology is not tangential/peripheral to the crime, such as electronic communications, which have become commonplace in numerous aspects of contemporary life. Otherwise cybercrime might incorporate virtually all crime. This is largely a return to the approach of Grabosky who appears in the first instance to have understood matters correctly.

In fact, in the current discourse on the topic, cybercriminal behaviours and activities vary widely and move well beyond hacking alone. They can include: online paedophilia, vandalism, harassment, espionage, fraud, activism, hobby hacking and cyberterrorism. Wall's (2001) typology, which has been widely applied by scholars, separates cybercriminal acts into four broad categories based on established crimes:

1. Cyber-*trespass* – crossing online boundaries into the computers and/or systems of others, possibly causing damage (e.g. hacking and viruses).
2. Cyber-*deceptions* and *thefts* – fraud/theft of money or property, such as credit card fraud or intellectual property violations.
3. Cyber-*pornography* – online activities that are counter to obscenity laws.
4. Cyber-*violence* – causing psychological harm to others, or inciting physical violence against them, such as stalking or hate speech (pp. 3-7).

This thesis focusses on cybercrime that involves an element of profit, as opposed to more malicious or political cyber-activities. Profit-driven cybercrime would mostly approximate the second category of Wall's typology. But in practice, such cybercrimes might straddle more than one category. For instance, hacking credit card data for profit might classify in both categories 1 and 2. Distributed denial of service

attacks (perhaps the closest cyber equivalent to violence), as part of an extortion campaign, could meet the requirements for categories 1 and 4 (as well as possibly 2). Furthermore, while many profit-driven cybercrimes do fit into category 2, it is also possible that some may not. One such example would be bulletproof hosting services which host cybercriminal enterprises online (such as phishing or pornography websites), but in return for payment do not remove illegal content even when directed to by various authorities. In such cases, there is a clear element of profit, but not necessarily a direct element of deception or fraud. In fact, an enormous money making industry has also grown up around online pornography (category 3), often linked to other types of cybercrime (such as hosting, internet traffic manipulation, spam and so on). As a result, profit-driven cybercrime could encompass every point in this typology.

Wall's typology is a useful starting point, but in practice for scholarly studies the motivations of cybercriminals may also be a useful categoriser. Among a broad range of perpetrators, there are five common cybercriminal "types": 1) those who are motivated by personal reasons, such as revenge against an old employer, a predilection for child pornography or harassment of an indifferent love interest; 2) recreational hobby hackers motivated by fun and/or intellectual challenge, but who intrude into networks or undertake other projects that contravene the law; 3) non-state actors driven by political ideologies, such as cyberterrorists or hacktivists; 4) profit-driven cybercriminals; and 5) nation-state actors and their affiliates engaging in cyber espionage against corporate, political, and military targets (Lusthaus 2014, p. 47). For the purposes of this thesis, there is a strong focus on the fourth category of profit-driven cybercrime. While there is some crossover, this category should be viewed as

quite distinct from other forms of cybercrime that persist, including hobby hacking, hacktivism or cyber espionage. These often (though not always) involve different actors and organisational structures, and as a result are not discussed in much detail as part of this thesis.

Who are the Cybercriminals?

This section addresses cybercriminal profiles. These issues are not directly addressed later in the thesis, but are mentioned here as important contextual background for the discussions on cybercrime that follow. The existing literature reveals little about this subject and so only a sketch can be provided. A large part of this is due to difficulties of access. This section addresses six key points: 1) the difficulty in developing a one-size-fits-all cybercriminal profile; 2) the distinction between cybercriminals and hackers; 3) an assessment of whether there is a link between cybercriminals and the autism spectrum; 4) the gender breakdown of cybercriminal offenders; 5) the age breakdown of cybercriminal offenders; 6) the motivations of profit-driven cybercriminals.

First, while it is tempting and practical to refer to "cybercriminals" as part of a discussion of cybercrime, it is wrong to assume that cybercriminals are a monolithic mass. In some sense, profiling "cybercriminals" is a lost cause. Just as cybercrime is a diverse phenomenon, so too are the offenders who carry it out. As will be discussed in chapter 4, there is a strong degree of specialisation within the cybercrime industry. Some offenders are hackers with strong technical skills, some are organisers who approximate (criminal) technology entrepreneurs, some have no technical skills at all

and for example might simply make ATM withdrawals with counterfeit cards that have been provided to them. These roles are but few among many, yet they demonstrate a basic point: with such diverse skill sets, it would be naïve to expect participants to conform to one profile. For instance, a career fraudster is likely to have a very different background from an elite hacker. It is beyond the scope of this section to go further, but rather than attempting to profile cybercriminals, a stronger approach is to break down clearly defined roles within the industry. Then one can assess whether common profiles might emerge based on those who carry out specific tasks.

This first point links closely to the second: not all cybercriminals are hackers and vice versa. *Hacking* is obviously an important term within the zeitgeist, but *hacker* did not have originally some of the negative connotations that it does today. The origins of hacking will be discussed in chapter 3, but, in short, students at MIT in the 1950-1960s were some of the early pioneers of it. In the early MIT days, a hacker was understood quite differently, as "someone who does some sort of interesting and creative work at a high intensity level. This applies to anything from writing computer programs to pulling a clever prank that amuses and delights everyone on campus" (http://hacks.mit.edu/Hacks/misc/faq.html). The nature of the early hackers demonstrates how far the meaning of *hacker* has shifted. It has become a contested term, often used in the media today to imply criminality, when it more accurately describes a skill set or personality. Hackers can have a range of motivations, leading to labels of white hat (good), black hat (bad) and grey hat (somewhere in between). One Western European hacker I met with as part of this study still viewed the term in a neutral way, despite also being a former cybercriminal who made considerable money from his activities:

> Hacking isn't about technology, it isn't about computers. It's about having a hacker's mindset. A mindset to understand things in a different way than other people. It doesn't necessarily mean that you all understand what you are saying. It just means that you are able to understand it differently, to stand out from the crowd. You are able to solve problems in a unique way. You are able to think differently. And usually when you've got that mindset you want to learn. Because without learning you don't know how to do these things (WE-(F)CC-1).

While cybercrime might involve hacking, the two descriptors remain distinct. Some cybercriminals are also hackers, but a number of others are not. In reverse, a great many hackers are not cybercriminals.

The third point addresses an ongoing debate about whether cybercriminals, or more accurately black hat hackers, have a specific psychological profile and a particularly high incidence of being on the autism spectrum. Other forms of economic crime have also attracted discussions as to whether offenders have a particular psychological profile different from the broader population (see, for instance, Babiak and Hare 2006). In the case of criminal hacking, specific reference is often made to social disorders like Asperger Syndrome (AS). The argument for a link between AS and cybercrime has gained some traction in recent years, but the evidence is far from clear. There are a number of high profile cases of cybercriminals that have either been diagnosed with disorders like AS or who have used such claims in their defence. The most famous of these is perhaps Scottish hacker Gary Mackinnon who hacked into US military systems leading to a protracted, though ultimately unsuccessful, campaign to have him extradited (The Telegraph 2009). Informal discussions with a number of prosecutors and law enforcement agents indicated that this issue resonated

strongly with some of them, with a number believing that AS was common among cybercriminals. Ledingham and Mills (2015) suggest a similar finding amongst law enforcement, but also note that currently there is not enough empirical evidence to strongly support such claims.

There appear to be two main points that would need to be addressed in this regard. One is to demonstrate a link between autism, or AS specifically, and technical ability or a hacking mentality. The second is then to demonstrate a specific link to criminal applications of those skills. Otherwise, it might be expected one might find a presence of those with AS among cybercriminals in similar proportions to other technical "professions". From the perspective of the fieldwork undertaken for this study, there was not strong evidence for AS claims. In many cases, those cybercriminals I met with were not socially awkward. They were personable and, in some cases, even charismatic. Of course, my sample is self-selective in that those who are interested in participating may be less likely to be socially awkward. There may also be something about the nature of profit-driven cybercrime that distinguishes it from other hacking activities, and does not attract to the same degree those who are on the spectrum. Many of those hackers and former cybercriminals I interviewed believed that strong social skills were important to the business and mentioned that they would be surprised if large numbers of autistic offenders were involved (SEA(E)-(F)CC-1).

The fourth point concerns gender. This appears to be one of the few factors that is consistent among cybercrime offenders. As one US law enforcement agent with undercover experience put it: "About the only profile that I can probably say is that they're male" (US-LE-2). This appears to hold true across a number of sub-disciplines

of cybercrime.[6] For instance, while there are some cases of female hackers, most of those arrested are male. As a result, I use male pronouns in general discussions throughout this thesis, unless specifically referencing a female cybercriminal. Interestingly, there are at least some aspects of cybercrime where women appear to play a key role. Cashing out is one such area. Some groups are largely male, but a number of others make extensive use of women. For instance, Chris Aragon who was the offline partner of leading black hat hacker Max Butler, employed a number of young women to buy expensive merchandise with counterfeit credit cards (Poulsen 2011). In a slightly different capacity, one cybercriminal I interviewed, Sean, used "drop girls" to provide addresses and receive the delivery of products that had been purchased with stolen funds (WE-(F)CC-1). Street gangs in the West Coast of America have also been known to make use of women, who might otherwise be engaged in prostitution, as part of their cashing out operations. This will be explained in more detail in chapter 8.

The fifth point concerns age. The traditional cybercriminal stereotype is of a very young offender, but this appears outdated and unrepresentative. Cybercrime encompasses a wide range of offenders, with a number of examples of actors in their 30s, 40s, 50s and even 60s. BOA, who was a leader of the influential CarderPlanet network (to be discussed in chapter 3), was in his mid-thirties at the turn of the millennium, despite many of his confreres being in their early twenties or teens. By some accounts he acted as a mentor figure to the group. At the further extreme, in 2016, 62-year-old Charles Eccleston pleaded guilty to attempting to infect US

[6] At the time of writing, the Cambridge Computer Crime Database, which collates offenders in the UK, indicates that less than 20% of offenders are female. The figure is likely even lower for professional cybercriminals, as the database also includes other manifestations of computer crime, such as misconduct in public office and breaching data protection laws which are likely to have a more equal gender distribution. The database can be found at: http://www.cl.cam.ac.uk/~ah793/cccd.html.

government systems with malware so that he could extract and then sell data to foreign states (USDOJ 2005). There are also other cases of those in this age bracket engaging in cybercrime, including John McHugh (aka Devilman) who was a member of the DarkMarket forum and was arrested for operating a "mini card factory" making use of compromised credit card data.[7]

But such a variation in age does not mean that the bulk of offenders is evenly spread. In fact, the demography of traditional forms of crime would suggest that most who are involved are in their teenage years through to their twenties (Hirschi and Gottfredson 1983, Cohen and Land 1987). It would not be surprising if cybercriminals fit a similar profile, but given the technical proficiency required, some of the more skilled offenders may be at the higher end of that range, having had more time to hone their craft and gain experience in the business. The range may also extend further. While a comprehensive global database of all known cybercrime offenders may help answer these questions, no such resource exists and it would be an immense undertaking. It would also fail to account for the ages of those many cybercriminals who have never had a brush with the law. That said, accounts based on partial databases from some jurisdictions suggest an average age of around 25 (Carignan 2015).

Ultimately, on this issue and others it is very difficult to come to a sense of the characteristics of offenders because datasets that would allow statistical analysis largely don't exist. For instance, my interviews with former cybercriminals also suggested a possible link between drug use and cybercrime. But this is only suggestive. The presence of drug users may be no higher than among broader criminal

[7] *R v Renu Subramanium and John McHugh*, Blackfriars Crown Court, 2010 [Opening Note].

populations, or the broader population. Clear statistics are required to compare the rate among the cybercriminal population compared to others. While some developments are occurring in this regard, a dearth of data remains one of the key difficulties in researching cybercrime. One of the main reasons for this is that surveys are quite difficult to carry out with a hidden population that has been quite small. In this study, it was challenging to access and then interview even a small sample of former cybercriminals. This approach also allows for a qualitative assessment of whether subjects are genuine cybercriminals or pretenders. For a survey, the sample would benefit from being much larger which presents a number of questions over access and also reliability (as to whether the participants are bona fide). Over time as the number of cybercrime offenders continues to increase, along with those who are convicted, such surveys may bear fruit. Continued attempts to build usable data sets are also a very valuable endeavour for the academy. But success in this area has not yet been reached and many questions relating to the nature of cybercriminals remain unanswered.

The final point under discussion is the motivations of cybercriminal offenders. In advocating for Routine Activity Theory, Cohen and Felson (1979, p. 589) suggest that "motivated offenders" are one key element of crime, alongside "suitable targets" and the "absence of capable guardians against a violation". Much of this thesis is focused on financial motivations for cybercriminal activities. Cybercrime appears strongly tied to aspiration and a lack of suitable employment options in a number of contexts. Given later discussions, I will not labour this point here. What is important to note is these types of rational and economic motivations need not exclude other reasons for involvement in crime. Humans are complex beings and other more "emotional"

elements likely also play a role among offenders. In conventional forms of crime, Katz (1988) focuses on the "seductive qualities" of committing particular offences. Throughout this thesis, there are moments where it is clear that cybercriminals may derive enjoyment or respond to other emotions when committing their crimes. For instance, in chapter 4 it is clear that some criminal hackers prize the intellectual challenge of undertaking their work, as much as they seek profits from it. It can deliver some form of rush. In chapter 7, an Eastern European cybercriminal illustrates that the profits made from criminal successes may not always be spent wisely. He makes clear that cybercriminals may enjoy "good times" seeking near total freedom: joyriding in expensive cars, drinking, taking drugs, clubbing, and having near constant sex. While noting these complexities in motivation, given the subject matter of this study, much of the focus of this thesis remains on financial motivations.

Literature Review and Theoretical Background

This section surveys the relevant literature on cybercrime, as well as theoretical background that might be useful to the questions at hand. The review itself is relatively short, given that writings on the subject of how cybercriminals have managed to cooperate and industrialise remain somewhat sparse. In fact, the broader social science literature on cybercrime more generally, while growing, is still relatively niche. As the spectre of cybercrime has risen over the past decades, scholarly interest in the topic has also developed. But the interest initially was from computer scientists and related disciplines: a technical subject area required a

technical analysis.[8] Over time, with the acknowledgement that there are human actors behind these threats, more social science based approaches on the topic slowly trickled into existence. Pioneers of this area have been writing on this topic mostly since the 1990s (see, for instance, Jordan and Taylor 1998, Wall 2001a), but in recent years, there has been a small flowering of a niche discipline of criminologists, sociologists and economists examining cybercrime (Lusthaus 2012, Hutchings 2013, Décary-Hétu and Dupont 2012, Holt and Lampke 2010, Mell 2012).

This growth in the literature is partly as a result of new forms of online data becoming available for analysis, but also mirrors the fact that cybercrime continues to grow as a major public and policy concern. Yet this budding field still has some way to go. Its content is only slowly moving into the "mainstream" and is yet to appear in the pages of many leading social science publications, beyond some respected criminology journals. And while the literature has begun to address some of the novel questions posed by cybercrime, it has only scratched the surface. A vast number of topics in the area remain unexplored and the sub-discipline is still determining the best tools to use in each case. This is certainly the case regarding issues of trust, cooperation and governance, which are central to understanding the growth of the cybercriminal industry. As such, this section begins with a review of the most pertinent cybercrime literature, but then moves to a discussion of relevant theory derived from the broader social sciences that should be more directly helpful in addressing the key concerns of this thesis.

[8] There are some rare computer science works investigating more human aspects (see, for example, Franklin et al. 2007, Furnell 2002, Motoyama et al. 2011).

Literature Review

The most relevant literature for this thesis is those studies that address the organisation of profit-driven cybercriminals. The field is not deep. There are some well known general overviews of cybercrime in book form (for instance, Wall 2007, Brenner 2010, Yar 2013), but these are focussed on cybercrime as a whole rather than specifically on financially motivated activities. One of the rare attempts to address this topic directly is Kshetri's *The Global Cybercrime Industry*, which provides an economics flavoured approach. While these works provide interesting conceptual insights, they all depend on the existing academic literature and open source material, rather than bring new data to bear on the subject. Given the deficit in general knowledge about cybercrime, such data is essential to a better understanding of the phenomenon. There have also been some good books on profit-driven cybercrime written by journalists, which often rely on a considerable number of interviews and extensive research (Poulsen 2011, Menn 2010, Glenny 2011, Krebs 2014). While they sometimes provide a useful sketch in passing, these books generally focus on the stories of specific cybercriminals, rather than paint a picture of the industry as a whole.

In terms of journal articles, studies on the organisation of financially motivated cybercrime have bloomed in recent years. This is partly driven by the availability of new forms of data, such as from publicly accessible trading forums, or those where anyone can register for an account (Holt and Lampke 2010, Holt 2013b, Décary-Hétu

and Dupont 2013).[9] Holt and Lampke (2010) qualitatively examine data from six publicly accessible trading forums and describe aspects of these markets including: the goods available; the payment systems used; the relationships between users; and the market dynamics. Decary-Hétu and Dupont (2013) use quantitiative methods to study the reputation index of an open-registration botnet-related forum, arguing that reputation is not randomly distributed, but rather tied to personal characteristics, networking and behaviour (see also Dupont et al. 2016). Holt (2013b) qualitively analyses a sample of threads from English and Russian language forums, by applying Best and Luckenbill's framework of social organisation, namely the key characteristics of: mutual association; mutual participation; division of labour; and extended organisational duration.

Such studies indicate some facets of the broader cybercriminal industry, but are often limited to discussions of online forums. As we shall see throughout this thesis, there is much more to the organisation of cybercrime than this aspect alone. And while these studies touch on issues of trust, cooperation and governance that might help explain how the growth of the industry has taken place, they rarely deal with these points in much detail. Those that do specifically address such concerns, appear more interested in the levels of trust within certain groupings, rather than in the specific mechanisms that lead to such levels of trust and subsequent cooperation among cybercriminals. For instance, Dupont (2014) examines the social organisation of a single hacking group, using logs of chats between the hackers provided by Canadian law enforcement. This allowed a rare analysis of private interactions of the group rather than just those the hackers were happy to publish publicly. While the hacking group

[9] A rare exception, which examined complete databases of forums that had been "leaked", is Motoyama et al. (2011).

in question is, by the author's own admission, far from an elite criminal operation, this study is commendable for providing a valuable window into the internal workings of such a group. Dupont does look at the issue of (dis)trust in the group, but his focus is not on specific mechanisms that increase trust. Instead, he provides an overview of various relationships in the group, the shifts over time in those relationships and why they occurred. Dupont highlights the need for further research in the area of trust, collaboration and cybercrime:

> The social capital that flows through such technology-mediated criminal networks also deserves much closer scrutiny. The scientific literature has, in my view, overestimated the ability and willingness of hackers to collaborate (Taylor 1999: 62, Schell et al. 2002, Holt 2009), assuming that the convergence of the global proliferation of available communication platforms, the semi-anonymity afforded by these technologies, and the jurisdictional boundaries constraining law enforcement agencies have eliminated the barriers that traditionally constrained illicit markets. However, far from creating a frictionless social environment for malicious hackers, these digital tools have a darker side that, under certain conditions, hinders collaboration and fosters distrust" (Dupont 2014, p. 211).

At present, there are only a handful of studies that have looked at the mechanisms of cybercriminal cooperation in any detail, and this subject has not always been the specific focus of these works (Holt 2013a, Motoyama et al. 2011, Yip, Webber, and Shadbolt 2013, Holt et al. 2015). These studies generally examine the key institutions for collective action found in cybercriminal trading forums, such as the power of forum officers to exclude/ban certain members, the provision of escrow services, along with feedback/rating systems allowing users to share information about past dealings. But because these studies only analyse data from forums, they cannot address the subtler interactions and aspects of cooperation that don't take place openly

on forums. These interactions could be outside forums because users choose to communicate further by more private means, as discussion becomes more sensitive, or because the cybercriminals in question choose not to join such forums at all. This is not to mention the cooperation that takes place offline, removed from cyberspace itself.

Furthermore, in addressing points of collaboration, stronger links could be made between the cybercrime literature and the broader social science theories of relevance, especially those that touch on trust, cooperation or governance and have been successfully applied in other criminal settings. The only study to have directly addressed matters in this way is a preliminary study of my own (Lusthaus 2012, 2013b). It was based on a small number of interviews in the United Kingdom with hackers, law enforcement, members of the technology sector and a former cybercriminal along with legal documents that contained examples of cybercriminal communications from the closed access forum GhostMarket. Like the examples above, this study addressed only online mechanisms, leaving aside discussion of mechanisms in offline settings. This is a common failing of much of the literature, with very little written on the offline dimension, especially with regard to issues of cooperation and governance. As such, the literature addresses only very specific aspects of the industry of cybercrime and its growth, and fails to address it as a unified whole.

This thesis is a far more extensive investigation of the cybercrime industry and the factors that help explain its growth. It draws on almost 6 years of field research and interviews with over 200 participants. It seeks to address a number of gaps in the

existing literature by: 1) demonstrating the value that fieldwork-driven qualitative studies can add to research on cybercrime, which is often focussed on novel forms of data rather than on more traditional social science approaches that are effective in studying "hidden populations"; 2) in more thematic terms, it aims to improve the overall knowledge of profit-driven cybercriminals and their industry at the "human" level, which still remains poorly understood; 3) as a core part of this analysis, it hopes to account for how the growth of the industry could be achieved when cybercriminals face significant challenges to cooperation, most notably when dealing with anonymous criminal partners.

Theory

In order to cooperate with one another and build a functioning industry, cybercriminals must overcome not only the risks of doing business with anonymous fraudsters, thieves and extortionists, but also the lack of any legal recourse for agreements to be enforced. Leaving behind the literature on cybercrime, broader social science theory might be relevant in helping explain the growth of the cybercrime industry. Issues of collaboration, cooperation, trust, institutions and governance have all been dealt with in some detail across a range of disciplines. But it is common for these approaches to have a rational choice or economics bent. While there is no uniform body of theory that can be drawn on, here I attempt to briefly pull together some of the key concepts that relate to successful collaboration/cooperation that will be relied on throughout this thesis. These include: trust; enforcement; institutions; governance.

In other criminal settings, trust has been suggested as a possible explanation for co-offending (McCarthy, Hagan, and Cohen 1998). It is not unreasonable in the cybercrime context to take trust as a starting point for investigations of cooperation. The first step in this process is to define trust and understand how it operates. As Dasgupta (1988, p. 51) puts it, trust is: "correct expectations about the *actions* of other people that have a bearing on one's own action when that action must be chosen before one can *monitor* the actions of those others". In a similarly influential formulation Coleman (1990, p. 91) sees the phenomenon as:

> an incorporation of risk into the decision of whether or not to engage in the action. This incorporation of risk into the decision can be treated under a general heading that can be described by the single word "trust". Situations involving trust constitute a subclass of those involving risk. They are situations in which the risk one takes depends on the performance of another actor.

It is important to distinguish here between the concepts of trust and trustworthiness. The problem of trust is that not everyone is trustworthy. In attempting to counteract this problem, mechanisms might be sought to make individuals more trustworthy, thereby reducing the risk involved in transactions (Hardin 2001). In terms of buttressing trustworthiness, there are three conventional mechanisms within that likely apply: *reputation*; *performance* and *appearance* (Sztompka 1999, ch 4). There is an extensive literature on the reputation mechanism in particular. In this regard, repeated interactions have regularly emerged as a key way in which reputations can be strengthened and cooperation enhanced, at least in small-scale interactions between few people (see Axelrod 2006, Klein and Leffler 1981, Abreu 1988). This could be achieved through building familiarity, incrementally testing compliance, but also by sanctioning the other side for defections. On the other hand, Schelling (1980, pp. 134-

135) saw matters differently, arguing that repeated interaction itself may actually incentivise cooperation:

> Trust is often achieved simply by the continuity of the relation between parties and the recognition by each that what he might gain by cheating in a given instance is outweighed by the value of the tradition of trust that makes possible a long sequence of future agreement. By the same token, 'trust' may be achieved for a single discontinuous instance, if it can be divided into a succession of increments.

But trust is not the only way in which cooperation can be achieved. Some forms of cooperation can also occur without trust. This ties closely to the concept of enforcement and related ideas such as monitoring and punishment. In simple terms one could closely monitor the actions of a partner to ensure that deception does not take place. But this type of activity could be very costly in terms of the time and resources required and in some situations it may not be possible. It is more likely to be effective when the burden can be shared by a group and information is transferred easily between them (Dixit 2004, Ostrom 1990). If the monitoring itself fails to encourage compliance, punishment may be applied. Within criminal circles, violence has traditionally been a favoured form of punishment, but others are also available. Sanctioning defectors may see them come back into compliance, but if the round of cooperation is already lost it might be more likely to deter future defection from the malefactor or others who take note of his/her treatment. Experimental research has found empirical support for punishment increasing compliance in later rounds of games (Fehr and Gintis 2007).

Another way of sidestepping trustworthiness is to place responsibility for a transaction in the hands of a third party. This then perhaps creates a new indirect problem of trust with that party. Third party enforcement can be carried out by the state or its endorsed agents, along with a number of extra-legal actors capable of performing similar functions in different contexts (Gambetta 1993, Varese 2001, Dixit 2004). The concept of third party enforcement is often known as a *credible commitment*. Cook, Hardin, and Levi (2005, p. 37) summarise matters in this way: "When there is no ground for trust, we can often establish reliability by demonstrating our commitment to take relevant actions. If we, whom you have no reason to trust, wish to convince you that we will be reliable in taking some action that will benefit you, we can try to establish a credible commitment". Along with third party enforcement, there are two famous game-theoretic examples of credible commitments that derive from the work of Thomas Schelling: *cutting off options* and *information hostages*.

The idea of cutting off options was originally explored by Schelling in his classic work *The Strategy of Conflict*. He outlined how limiting one's own options can lead to a strange paradox where: "weakness is often strength, freedom may be freedom to capitulate, and to burn bridges behind one may suffice to undo an opponent" (Schelling 1980, p. 22). Schelling later settled on an historical example to bear out his point with the example of the Greek general, Xenophon. When facing the Persians, Xenophon chose to position his army with its back to a ravine. His view was that the enemy could flee in any direction, but by cutting off options the message to his troops and their opponents was that the Greek army was now bound to fight and to win. For

Schelling such a "commitment" could thereby influence another's choices (Schelling 2006, p. 1).

Schelling's concept of information hostages is perhaps even more relevant to the case of cybercrime. This idea approximates the historical exchange of hostages in order to strengthen relationships and avoid conflict. But in this case compromising information rather than people are swapped, which enhances cooperation by giving each individual the power to incriminate the other if there is a defection. Schelling provides one hypothetical illustration in this way:

> Both the kidnapper who would like to release his prisoner, and the prisoner, may search desperately for a way to commit the latter against informing on his captor, without finding one. If the victim has committed an act whose disclosure could lead to blackmail, he may confess it; if not, he might commit one in the presence of the captor, to create the bond that will ensure his silence (Schelling 1980, pp. 43-44).

Gambetta extended Schelling's idea, suggesting that "deviant" groups could reinforce internal loyalty by having members exchange evidence of their past misdeeds (Gambetta 2009a, p. 66). Campana and Varese (2013) examined two traditional organised crime groups (OCGs), finding that kinship and shared information about violent acts could help buttress trustworthiness and illicit cooperation.

Online paedophile groups are suggestive of the possible applicability of information hostages to profit-driven cybercrime. Such groups appear to form largely in order to share child pornography materials online. Gambetta (2009) outlines how such paedophiles require various tests of commitment, along with proof that one is not a

law enforcement agent, to join their groups. One such test was the provision of ten thousand original pornographic images. But a stricter test was that certain members travelled to other countries to vet would-be recruits face to face. The primary significance of this was that when "identification is at a premium and must be kept secret, just showing one's face is itself like giving a hostage, namely the knowledge of one's key sign of identity" (Gambetta 2009a, pp. 62-63). It might be expected that some profit-driven cybercriminals, very distrustful of other collaborators, might vet potential collaborators they have met online in a similar way, choosing to meet face to face in a specific location.

So far, the focus has been on trust and enforcement. It is clear how these elements can contribute to cooperation, especially on a small scale. An individual can assess the trustworthiness of a potential partner and act accordingly. They can also seek to enforce matters themselves or rely on a trusted figure to provide third party enforcement. But difficulties emerge if one wishes to expand trade by moving beyond the small scale and begin to collaborate with, for instance, strangers whom you know little about and who might disappear before a deal can be enforced.[10] In his extensively cited paper *Institutions*, Douglass North summarises the problem in game-theoretic terms:

> Wealth-maximizing individuals will usually find it worthwhile to cooperate with other players when the play is repeated, when they possess complete information about the other player's past performance, and when there are small numbers of players. But turn the game upside down. Cooperation is difficult to sustain when the game is not repeated (or there is an endgame), when

[10] The difficulties of scaling cooperation from small groups to larger ones are well known (see, for instance, Olson 1971).

> information on the other players is lacking, and when there are large numbers of players (North 1991, p. 97).

In order to understand the development of a large industry, such as cybercrime, something more is required. Cybercriminals come from all over the world and, online, nothing is known about them unless they choose to reveal it. There are many of them and they sometimes wish to collaborate with a partner for one deal only. For the challenging examples that Douglass North examines, the solution is the concept of *institutions*, which he defines as follows:

> Institutions are the humanly devised constraints that structure political, economic and social interaction. They consist of both informal constraints (sanctions, taboos, customs, traditions, and codes of conduct), and formal rules (constitutions, laws, property rights). Throughout history, institutions have been devised by human beings to create order and reduce uncertainty in exchange (North 1991, p. 97).

The key mechanisms relating to trustworthiness and enforcement still drive cooperation, but it is effective institutions that enhance the operation of these mechanisms and allow them to be scaled. Institutions lead to an overall ordering of interactions and reduce the costs involved in exchange. Without them, it would be difficult for actors to move beyond dealing only with those that are well known to them and with whom agreements can be relatively easily enforced.

This discussion of institutions links with the final point on governance. These two concepts are closely linked, as those who provide governance are often responsible for the creation and management of institutions. In general theoretical terms there are two ways in which such a system of governance can emerge. One is a top-down

manner where order is imposed by a hegemon, as classically stated by Hobbes (2012 [1651]). The other way is bottom-up, whereby order evolves spontaneously and without design, arising to meet needs among humans but not always in predictable ways (see, for instance, Hayek 2006, 1988). A related division can be found in discussions of extra-legal governance, where alternative modes of economic governance are developed in situations in which the state is unable to effectively protect property rights and enforce contracts. Dixit (2004) provides an overview of this broad topic area, arguing that there are two alternative organisational structures that can (at least partially) take the place of the state: self-governance and private governance. Akin to a bottom-up approach, self-governance suggests that order can emerge and be maintained within a group as long as communal punishment options are present, and information about members cheating each other can be transmitted across the group. In top-down terms, private governance involves paying third party individuals or groups to enforce contracts and provide protection for property rights.

In relation to criminal groups, private governance has played a key role in the literature. In fact, for a certain school of scholars, the concept of organised crime is built around governance. Thomas Schelling's key argument is that organised crime is not simply "crime that is organized" (Schelling 1971, p. 72). In explaining his approach, Schelling provides the famous account of why organised burglars do not fall into the category of organised crime:

> burglars are never reported to be fighting each other in gangs for exclusive control over their hunting grounds. Burglars are busy about their burglary, not staking claims and fighting off other burglars. It is when a gang of burglars begins to police their territory against the invasion of other gangs of burglars, and makes interloping burglars join up and share their loot or get out

> of town, and collectively negotiates with the police not only for their own security but to enlist the police in the war against rival burglar gangs or nonjoining mavericks, that we should, I believe, begin to identify the burglary gang as organized crime (Schelling 1971, p. 74).

In this conception, genuine organised crime groups attempt to regulate and control some form of illegal industry. This approach is central to definitions of organised crime and mafias that Varese (2010) settles on, after surveying the range of definitions that has been applied to the subject. Varese defines an organised crime group as one that "attempts to regulate and control the production and distribution of a given commodity or service unlawfully". Drawing on the work of Gambetta (1993), he defines a mafia as a type of organised crime group that "attempts to control the supply of protection" (Varese 2010, pp. 14, 17). This effectively means that a mafia seeks to govern all criminal industries.

This governance-centric approach is in line with empirical evidence on the subject. Perhaps one of the best explanations of what a mafia is comes from Henry Hill, the gangster whose biography became the inspiration for Martin Scorcese's film *Goodfellas*. In Nicholas Pileggi's *Wiseguy*, Hill outlines the role performed by Paul Vario, the local area *Capo* of the Lucchese crime family:

> The guys who worked for Paulie had to make their own dollar. All they got from Paulie was protection from other guys looking to rip them off. That's what it's all about. That's what the FBI can never understand – that what Paulie and the organization offer is protection for the kinds of guys who can't go to the cops. They're like the police department for wiseguys (Pileggi 1986, p. 48).

One of the key points of interest in this thesis is whether cybercriminals have achieved this level of governance in their dealings and whether this has contributed to the overall success of the industry. Also to be examined, is whether traditional organised crime groups like mafias are involving themselves in cybercrime and providing a degree of governance themselves.

This subsection has brought together theoretical background that might help explain how cooperation can be achieved and enhanced on a broad scale. It has argued that trust and enforcement play a key role, but that in order to scale their impact institutions and a system of governance will likely help. The more established and efficient these mechanisms become, the greater levels of cooperation there should be. But it is naïve to think that cooperation will become universal. Even within societies with strong institutions and governance, some defection will take place. Formal contracts and legal systems to enforce them reduce the risks involved in transactions. There are also more informal means that might be employed such as relying on past interactions to determine trustworthiness (Axelrod 2006, Gibbons 2001) or reputation systems that can disseminate information on those you haven't met directly (Cook et al. 2009). But even with such mechanisms, some element of risk will always remain. Court systems may not function efficiently or transparently in various jurisdictions or a partner that one has dealt with over a number of years might suddenly disappear with a large sum of money.

Given the fundamentally distrustful environment of cybercrime, the expectation is that these actors will also face defection, probably to a much higher degree than in transparent and functioning societies. After all, they are not only dealing with

criminals, but they are often dealing with anonymous strangers as well. This further weakens trust and any available enforcement options, thereby increasing the risks. But in order to establish the industry that cybercriminals have, they must have managed to find ways of minimising these risks. The theory described in this subsection offers a strong starting point for investigations into how this success has been achieved. It will be drawn on throughout this study.

Approach and Structure

This thesis is focussed on addressing two key issues. First, it argues that cybercrime has evolved into a sophisticated profit-driven industry. Second, it seeks to understand how this evolution has taken place when anonymity and other challenges would suggest that cybercriminals are more likely to operate alone or in small groups. The approach undertaken in this thesis is strongly qualitative and also exploratory. In effect, it is entering largely uncharted waters and seeks to draw a map of the cybercrime industry and how it functions. The theory described above offers some useful hints so as not to become lost in this expanse. But with that said, much of its contribution is empirical, offering new insights into cybercrime and aiming to provide a detailed overview of the subject based on almost six years of field research. As such, this study cannot be packaged to fit neatly into popular academic distinctions, such as empirical versus theoretical, deductive versus inductive, explanatory versus interpretivist. It should rather be seen as a first step that explores what is an immense if often hidden world. Perhaps, following this study, it will be easier to read the map and engage in some narrower and more tightly defined investigations that fall within these distinctions. In the meantime, no apologies are made, but the next chapter

includes further discussion of this point.

As to the structure, the thesis begins with a chapter on data and methods, which outlines how the study was undertaken. The following two chapters address the first point of how cybercrime has evolved into an industry. Chapter 3 outlines the history of profit-driven cybercrime; chapter 4 offers analytical insights that make sense of the topic within the framework of industrial organisation. The remaining four body chapters address the second point of how this industrialisation has taken place when facing the challenge of anonymity. Chapter 5 addresses how cybercriminals establish an online identity through the use of nicknames, a foundational point before any cooperation can take place. Chapter 6 investigates what mechanisms cybercriminals employ to enhance cooperation online. Chapter 7 attempts to explain why some cybercriminals seek to collaborate offline and how this helps strengthen the industry. Chapter 8 assesses whether there is now a degree of offline governance aiding cybercriminal cooperation, whether provided by organised crime groups or otherwise.

2. Data and Methods

This chapter outlines the key data and methods used for the thesis. The first section addresses the research style adopted for the project. The second section outlines the key data sources and their collection. The third section discusses the scope of the study, including aspects of sampling and limitations. The final section addresses important ethical considerations.

Research Style

This study makes use of qualitative methodologies. A lack of credible cybercrime statistics limits conventional quantitative work on the subject. Some scholars have found creative ways to carry out quantitative studies, which often require coding cybercriminal communications from law enforcement data or data which has been scraped from open source or leaked forums. But for the present study, a qualitative approach is more appropriate. First, cybercrime is still a poorly understood phenomenon, with few details known about a number of its aspects. A broad qualitative study allows a more comprehensive understanding of the industry of cybercrime and how issues of cooperation function within it. In fact, it might reveal possible approaches and further research directions for future quantitative studies of these issues. The thesis is also focussed on the mechanisms that cybercriminals have developed to enhance cooperation and establish a functioning industry. Mechanisms remain something that qualitative work is well suited to addressing and something

that can be a challenge for quantitative approaches, which are often better suited to determining correlations.

As flagged in the introduction, the core approach of this thesis is *exploratory*. It cannot be easily categorised within some common academic distinctions, such as: empirical versus theoretical, deductive versus inductive, explanatory versus interpretivist. I have always approached this project as an exploration, but over the course of the research I have had academic input from various quarters encouraging me to fit into one of two boxes. Box one could be summarised as focussed on hypothesis testing. It draws on existing theory and is centrally interested in what the case of cybercrime might tell us about that theory and about other non-cybercrime cases where similar issues are faced. By employing hypotheses it relies on deductive logic to test them. This is an approach most familiar to quantitative researchers but can be applied successfully to qualitative work, as perhaps most clearly outlined by King, Keohane, and Verba (1994). Box two is a more anthropological approach, ethnographic and strongly empirical. It begins with the fieldwork and data and uses inductive logic to work backwards into developing potential theory. But its focus can be very much on a particular group under study rather than attempting to generalise broadly with regard to natural laws (on anthropological/ethnographic approaches see Bernard 2011, Maher 1997).

While I have attempted to fit my research into both these boxes at particular points, it ultimately seemed to be a futile exercise. In terms of box one, the main challenge was developing testable hypotheses. The scope of this project is wide. Despite my undertaking years of fieldwork, the type of data remains largely suggestive. Although

a substantial qualitative sample, 200 interview participants are but a fraction of the cybercriminals, law enforcement agents and technology sector employees engaged in this area. While I reached saturation and began towards the end of the study to hear subjects repeat similar points, further work may unearth new findings. This is mostly due to the wide variation in the sample, which is not a surprise given the cybercriminal specialisation and geographical disparities that will become apparent. Any attempt to address a specific hypothesis would often fail, because the data did not speak with one voice. While hypothesis testing can be carried out with qualitative data, it requires a much narrower research agenda, most likely focussed on some key case studies so variation can be limited, data contained, and the hypotheses stated in a more specific way (see, as an example, Varese 2011). The scale for this project is simply too large.

But just because box one didn't apply, does not mean that box two was more appropriate. Ethnography conventionally employs inductive reasoning, drawing together insights from a rich description of a culture that leads to theoretical suppositions. This thesis employs a different approach, beginning with key theory and research questions to be investigated through the collected data. From the beginning of this study, there has been one key research question I have sought to investigate, which was derived from the body of theory on cooperation and governance, particularly those texts relating to crime and extra-legal groups (Dixit 2004, Gambetta 1993, 2009a, Varese 2001, Schelling 1980). When applying this mode of thinking to the idea of online crime, a puzzle quickly emerged: how do cybercriminals successfully cooperate when dealing with anonymous criminal partners online? As noted in the introduction, one would expect trust to be difficult to attain in such

circumstances, yet a large cybercriminal industry has evolved. While I don't employ hypothesis testing, I have had a clear theoretical focus from the outset and have undertaken fieldwork with this central question in mind. This interest has also been very much linked to broader theory, rather than addressing cybercrime as a more isolated case.

While perhaps delving into secondary issues, the research methods employed in this study also differ from conventional ethnography. The key point is that I did not embed myself within a specific community in order to observe behaviours and practices. The development of online communities has led to the birth of online ethnography, which allows researchers to engage virtually with these communities from the comfort of their own surrounds. But this approach is not made use of in this study for a number of reasons. First, some data from archived forums and other meeting places is already publicly available which paints a picture of some of these communities without having to take on the complications of dealing with them directly. Second, there are a number of ethical issues involved in studying these groups, related to notifying one's role as a researcher, whether and when informed consent needs to be attained, and also to any barriers to entry to joining such groups. These latter tests become increasingly pronounced when attempting to engage with the more elite and secretive actors, and may require evidence of criminality to build trust. This is something academics cannot do, unlike undercover agents from government or perhaps even the private sector, who have their own methods to provide this evidence. Ironically, a focus of the study – mechanisms to weed out non-criminals – becomes a key ethical challenge for academics to engage with participants online. Finally, and most importantly, even if one can access participants online and

they agree to be interviewed, the interview is effectively with their online persona rather than their offline self. These can be very different people who provide very different perspectives. This is coupled with the dangers of interviewing active criminals who may have an incentive to lie or hide aspects of the truth.

Instead of taking such an online approach, this study is built around conventional offline fieldwork. But this still does not fit within the ethnographic model, which is focussed on participant observation. For the present study, fieldwork centred on meetings where interviews took place. While some observation of interview subjects occurred during these meetings, and broader observation of the countries and cities that I visited were extremely beneficial for understanding context, the interviews themselves were always the primary data source. The ethnographic approach is often centred on the depth of information that can be attained about a specific group. While this can be done comparatively, the time and resources required often limit the number of cases that can be included (for a rare exception see Sanchez-Jankowski 1991). The focus of this study is on breadth rather than depth. It is effectively a study of variation. A core part of this was the need to piece together and to comprehend the complexity of the global cybercrime industry, which exists in many countries and therefore leads to inherent differences.

The approach adopted in the thesis draws on elements found in both the theoretical/deductive/explanatory and empirical/inductive/interpretivist camps. But it subscribes to neither of them. It is led by theory and a specific research question, but does not engage in hypothesis testing. It involved extensive data collection, but is not an ethnography of a group. It has a specific interest in the case of cybercrime, but also

what this case can tell us about existing theory. It cannot be fitted neatly into either category because it is exploratory in nature. It is an early voyage into largely uncharted waters. Once more is known about cybercrime, studies that fit neatly into these categories could be more easily undertaken. But at this stage, the focus is on better understanding the topic and effectively drawing a map of this new world.

Data Sources

The thesis draws on four main forms of data. First, it makes use of legal documents, such as indictments. Second, it draws on various communications between cybercriminals, such as forum screenshots and archives. Third, it incorporates relevant open source material, such as media articles on cybercrime and interviews with cybercriminals. Finally, and most importantly, the core data source of the study is over 200 interviews carried out since 2011 with law enforcement agents, members of the technology sector, former cybercriminals and others with a detailed knowledge of the subject.

The legal documents were largely those from the public sphere and are often publicly accessible. For instance, US indictments and other documents associated with cybercrime cases are often publicly listed by the Department of Justice. Some of those which have not been published by the government have been made available by journalists and others. In the UK, similar documents are not as easily available. The closest equivalent is prosecutorial opening notes, which present similar information to indictments. These are often not published in the same way, but can be obtained by purchasing court transcripts or from prosecutors themselves. Finally, I obtained some

material from officials/agents that was not in the public domain or accessible to the general public, but which provided important detail on certain cases.

US and UK documents formed the bulk of records analysed. Both countries are active in cyber law enforcement. In particular, the US engages with a number of major international cases involving offenders from a number of jurisdictions. Unfortunately it was not possible to access such legal records across many jurisdictions included in this study, as this would have involved an extensive investment of time and resources that was not possible in the scope of the project. Numerous language barriers and bureaucratic hurdles posed key challenges, which would be difficult to overcome unless one were engaging in a case study of a specific jurisdiction.

Another valuable data source was screenshots, logs and archives of cybercriminal meeting places and communications. This allowed an analysis of cybercriminals speaking to each other in the wild. As mentioned above, this did not need to be accessed from active forums, as there are many screenshots and (partial) archives of cybercriminal forums available online. Some forums are now defunct, while others have suffered leaks but may continue to exist. The Wayback Machine also offers snapshots of the historical Internet, allowing some idea of forums that were not otherwise well archived. There were also screenshots contained in the legal documents mentioned above. Some individuals also furnished me with forum archives from the past, or with logs from chats they had participated in.

There are also numerous open source materials available that make for useful data. These include published interviews that have been carried out with active or former

cybercriminals, as well as biographical and autobiographical accounts of cybercriminals published in books and articles. There is also a growing number of media articles tracking cybercriminal cases, organisations and endeavours. Some of the best of this work comes from those who are themselves embedded in cybercriminal communities or have strong relationships with active sources.

Finally, the fundamental data source of this project is the semi-structured interviews that I carried out at different points with over 200 participants, starting from 2011. Interviews are better suited to investigating sensitive topics than more impersonal surveys (Brannen 1988p. 553, McCracken 1988, pp. 9-11). Given the difficulty in accessing participants, it is also important to extract as rich information as possible from those who do participate. For the interviews, there was a range of subjects with a strong knowledge of cybercrime coming from a range of backgrounds. But most participants fit within one of three categories providing distinct perspectives: 1) former cybercriminals; 2) current and former law enforcement agents; 3) technology sector employees. Some people fitted within multiple categories, such as former cybercriminals or former law enforcement agents who now work in the private sector. The next section covers how participants were selected for interview, how they were approached and sampling issues therein. A list of all participants is found in the appendix. Overall, I interviewed 12 admitted or known former cybercriminals.

All the field visits in this study followed the same model. They were short, ranging from a few days to a few weeks, and scheduled well in advance to include as many interviews as possible. Many interviews were arranged before my arrival, while a smaller number were arranged on the ground sometimes with the help of other

interview subjects I had met. As noted above, the purpose of these trips was to gather as much data as possible in the form of interviews in each location, rather than to spend considerable time in a location and build a thick ethnographic description of a specific community. Generally two interviews were scheduled each day. Sometimes three were undertaken, sometimes only one. There were only a handful of occasions where I failed to secure any interview on a specific workday. There were surprisingly only a handful occasions across the project where an interview subject failed to attend a scheduled meeting.

I met with most participants in person. Some could not meet in person, due to scheduling or geography, or preferred not to meet in person, due to concerns of privacy or other reasons. In these cases interviews were conducted either over the phone, or online equivalents, or through electronic communication like email or chat. Most participants took part in a formal interview which was centred on a set of core questions that I had developed, but often ranged into other areas according to the knowledge/interests of the participants. In many instances, these interviews were taped using a voice recorder I carried with me. When participants preferred not to be recorded, I most often took notes. After such meetings concluded, I would flesh out the notes based on my recollection of the interview. This would usually occur within the same day as the interview, or in rare cases where my schedule didn't allow, within a couple of days. I also took these opportunities to record observations about other meetings that were recorded, along with my general observations about the locations I was in. This centred on contextual details, like economic or cultural factors, that I thought might be relevant to the cybercrime situation locally.

Other researchers have noted that recording interviews can lead to evasive answers (Varese 2001, p. 12). This was primarily the reason I offered a choice at the beginning of interviews, which served to be a very effective strategy. A significant number of participants chose not to be recorded and I presume they were more forthcoming than they otherwise would have been. At times this choice appeared to be partly influenced by culture or local norms. For instance, in Hong Kong no local citizen wished to be recorded. But, given the sensitivity of issues involved, I was somewhat surprised by the high proportion of those who were willing to be recorded elsewhere around the world. A number even preferred to be recorded, as they wished to make matters easier for me as a researcher or wished that their points be captured more accurately. Some would request the recorder to be turned off at certain moments when they wanted to divulge something they didn't want on the tape. There was even a high proportion of former cybercriminals who were happy to be recorded, despite their information perhaps being the most sensitive. This might have been due to the open nature of cyber actors, mirroring the utopian ideals online of information sharing and a lack of boundaries. Perhaps it was for other reasons. Overall, recorded interviews often proceeded more fluidly, the conversation flowed and often the recorder was hardly noticed (for similar arguments see Legard, Keegan, and Ward 2003, pp. 166-167). Note taking was often an obstruction and slowed discussions down, and may have served as a regular reminder of the formality of the meeting.

A smaller number of participants elected to have an informal discussion. This may have been due to a number of reasons, but often these participants were happy to assist yet wished for a further barrier between them and the official research output. The comfort of subjects was the primary focus so I would always acquiesce to such

requests. I would also usually offer the informal discussion option to those who had agreed to an interview, but who I believed had some sensitive issues related to their case. For instance, in some jurisdictions legal professionals don't publicly state their views on particular matters. I often took notes of these conversations, but used this information for background. I make note of those who participated in this way in the appendix, along with all other participants. But I do not directly cite these informal subjects with regard to particular pieces of information they provided.

Once the data had been gathered, I outlined key topics of interest to the research question and the structure of the thesis. I then coded the data accordingly and grouped the relevant data points together in order to write them up. These topics fell in line with the eventual chapters of the thesis with key markers including: history; organisation; nicknames; online interactions; offline interactions; governance (organised crime/corruption/state connections). Once this initial division was made, the data was then sorted under the subsections that appear in each chapter.

Scope, Sampling and Limitations

One of the main challenges in undertaking this study was defining the scope. Cybercrime is a vast subject area. The internal boundaries that lie between different groups and activities that fall under this banner have not been clearly demarcated. This made it difficult to choose case studies as an approach as there was not much evidence to identify and then justify the choice of specific cases. One could have chosen certain forums or countries to focus on, but there was not a clear idea of where these cases fitted into the broader economy of cybercrime. In fact, a very significant

component of fieldwork in this project involved gaining a far more detailed and nuanced understanding of cybercrime than is currently present in the literature. This context was essential before it was possible to address the research question on the topic of cybercriminal cooperation and industrialisation. But it also may make a broader contribution in helping to identify what groups, countries or otherwise may serve as suitable case studies in future projects.

My thinking on the subject of case studies has evolved, as my understanding of cybercrime increased. In the early days, I believed that case studies were not possible with regard to cybercrime as it was such a transnational phenomenon with anonymous actors meeting online that were difficult to track. But I have now revised this view. It seems that fruitful case studies could be carried out on specific cybercriminal groupings, by drawing together data on these cases and seeking to interview those with a specific knowledge of the group in question. While the transnational nature of these groups may make the data collection more challenging, it remains possible. When more than one group is working together, one would also need to determine where one group ends and another begins. It might also be rewarding to engage in case studies of countries or smaller geographical units in terms of the cybercrime issues found there. There appears to be significant variation in styles of cybercrime depending on the region, country or even place in question. One could benefit from gaining a better understanding of the specific flavour of cybercrime found in such contexts.

This case study approach is not adopted here. This is partly because I identified suitable cases only by having completed this project in the first place. But the

approach in the thesis is also intentionally broad by design. It seeks to survey profit-driven cybercrime as a whole, with its central focus on answering the key research question of how cybercriminals have established a functioning industry. As part of this, it brings in theoretical assumptions to be applied to the case of cybercrime. This theory cuts across many aspects of cybercrime, and humanity as a whole. As such, it is the variation (or lack thereof) between manifestations of cybercrime that is of central interest. And rather than being limited to one or two cases of cybercrime, a much broader approach allows significantly more variation. This offers a more nuanced investigation of how cooperation works and fits within the broader world of cybercrime.

Geographical Sampling

Sampling for this study involved two elements: 1) as I couldn't carry out fieldwork in every country in the world, choices had to be made on which geographies to focus on; 2) there was also a number of sampling questions with regard to how interview subjects were chosen. To begin with the question of geography first, this aspect of sampling evolved over the course of the study, largely due to the knowledge that I developed along the way. The first phase of this project began in 2011 with a small study of cybercrime in the United Kingdom, which constituted my masters dissertation and effectively served as a pilot for this current work. One of those early participants offered a view that was not widely challenged by other subjects: that cybercrime was a universal phenomenon that didn't differ significantly between countries. In research following this pilot, this became an early supposition that I

tested, as I continued to investigate the central research question and to gather background information.

Phase 2 effectively involved visits to countries that were somewhat chosen at random. This might be viewed as a form of accidental, opportunistic or convenience sampling (Maxwell 1996, Burgess 1984, Honigmann 1982, Hoyle, Harris, and Judd 2002, p. 186). These were often places that I was passing through or visiting for other purposes where I took some time to carry out fieldwork. Given the supposition that cybercrime was the same in each country, the specific choice should not matter. The first country visited following the UK was Singapore. This case immediately challenged the idea that cybercrime was the same everywhere because there appeared to be very little evidence for local cybercrime other than a small number of very minor cases. This is perhaps unsurprising given the low rates of crime in Singapore in general which appears partly due to economics, but also to strict laws and punishments and a subsequent culture of obedience that emerged from this. Other countries that I conducted fieldwork in during phase 2 included: Australia, Hong Kong; Malaysia; Switzerland; Thailand and some other parts of Europe that are redacted for the protection of certain participants. During this time, I also carried out work in the United States, but the reason for this visit falls more within Phase 3, which will be discussed below.

Visiting these countries was essential for understanding the variation involved in cybercrime, contrary to my pilot findings. Due to the fact that many of these countries were not cybercrime hotspots, strong positive findings relating to the research question were often limited. But this was not necessarily undesirable and contributed

to the overall strength of the study in a number of ways: 1) The data collected here served to improve my understanding of cybercrime. Even if the local cybercrime situation were not severe, a number of global experts on cybercrime nonetheless happened to be located in these countries. These countries also provided important variation in the sample: those cases where cybercrime is not prevalent can help shed light on what is distinct about those jurisdictions where cybercrime is a major challenge; 2) through expert opinion, research in these locations helped identify those cybercrime hotspots that were essential for me to visit as part of my study (to be discussed below); 3) related to point 2, due to a lack of strong positive findings these visits helped to confirm that expert opinion and the literature had not missed some key cybercrime hotspots that had been overlooked in the discourse; 4) finally, there were some surprises in these locations that made them worthwhile research ventures. In some locations I found high value interview subjects, such as former cybercriminals who happened to be residing in these jurisdictions but were not necessarily from there in the first place. In other instances I made unexpected discoveries, such as the physical presence of a significant number of Nigerian scammers in Malaysia. This was a phenomenon that I was then able to track throughout other countries.

The third and final stage of the project involved a concerted effort to visit cybercrime hotspots. These were locations that previous expert opinion had identified as being significant hubs of cybercrime. These were often believed to have a high concentration of cybercriminals. These locations included Russia (2 visits), Romania (2 visits), China, Ukraine and Nigeria. These were not the only hotspots mentioned in previous interviews, but the time and resources required did not make it feasible to visit all of the places that were mentioned. For instance, other former Soviet bloc

countries, such as Belarus and Moldova, are also linked by some to large-scale cybercrime. But it was Russia, Ukraine and Romania that were chosen because they came up most often throughout interviews as holding a central place within Eastern European cybercrime. Such views were also supported by known cases and public source material. In most cases the depth and quality of data I obtained in these locations bore out the expert opinion. The only exception was China, which occupies a key place in the mind of those in the cyber security field due to the large number of cyber attacks associated with it. But one of the key discoveries there, is that the cybercriminal sphere is relatively immature. The main activities appeared to relate more to cyber espionage. Perhaps for many on the outside, the distinction can be difficult to draw when they simply see attacks coming in but don't always have a sense of the perpetrators and their motivations.

There were also countries that I chose to visit for other specific reasons, such as to meet certain people of interest. For instance, both the United States and the Netherlands have their share of cybercriminals, but they are also leading hubs for law enforcement agencies and security companies. I visited them to ensure access to both these groups. In certain cases, I had a specific thematic reason for visiting some countries based on tips and suggestions from earlier interviews and meetings. In Latvia I tried to examine connections between cybercrime and money laundering. In India, I was investigating a possible connection between cybercrime and Indian call centres. In both cases, I did not find strong positive results, but for other reasons the trips proved useful.

I also had to make strategic choices within countries that I visited. I focussed on cities and towns that were known hubs of cybercrime. This often included a capital or major city, such as Moscow, which served as a useful way to access law enforcement agents and technology companies that are often located in these centres. I also targeted more regional cybercrime hubs based on past interviews and background research. For instance, in Romania I visited the infamous online fraud centre of Ramnicu Valcea, in addition to spending time in Bucharest. In Ukraine, along with carrying out interviews in Kiev, I made sure to visit Odessa which plays an important role in the history of cybercrime. But budget, time and other practicalities also limited my going to further locations. For instance, in Nigeria I based myself in Lagos but was not able to visit other hubs due to budget and time restrictions. In Ukraine, I could not visit Donetsk due to the ongoing conflict in the east, but felt that sufficient data was gained in Kiev and Odessa alone.

Though chronological, these phases should reflect shifts in research strategy, rather than strict delineations in time. For instance, I visited the United States while still undertaking phase 2 research in places like Thailand. I also continued to carry out research in the United Kingdom throughout all the phases as a result of being based in the country.

Purposive Sampling

The other key aspect of sampling for this study relates to the participants themselves. This project made use of both purposive and snowball sampling. Having no prior contacts in the area at the beginning of the project, it began with purposive sampling

(Ritchie, Lewis, and Elam 2003, pp. 78-80, 96-104, Hoyle, Harris, and Judd 2002, pp. 187-188). In fact purposive sampling remained the key approach even later in the study when some snowballing was possible (this was due to some key weaknesses in the latter style with regard to this study, which will be explained in the subsection below). From the outset, I was interested in interviewing those with a strong knowledge of cybercrime from a range of backgrounds. Over the course of the study I talked to former cybercriminals, hackers, law enforcement agents, lawyers, government officials, international civil servants, NGO employees, journalists, private sector cyber investigators and cyber intelligence practitioners, security company employees, banking and financial institution employees, and engineers.

Early on I identified that there were three clear categories that were most relevant for my study: former cybercriminals; law enforcement agents; and those in the technology sector with a focus on cybercriminals. These are the groups that have the strongest connection to cybercrime. Yet I also learned the lesson that some meetings can be unexpectedly useful and I continued to set meetings with some outside these core groups if I thought they might have a strong knowledge of the area. The general rule was that those with a direct knowledge of cybercrime were the most valuable subjects in closely answering my research question. Former cybercriminals obviously have a detailed knowledge of how cybercriminals operate. I chose to focus on former rather than active cybercriminals for a number of reasons: they have less reason to lie about their criminal behaviour as it is in the past; they are often easier to locate in person or otherwise; the risks of any danger to the researcher are lessened; as are the risks of being caught up in an ongoing law enforcement investigation.

Some clarification is important to include here. It is not the case that I chose not to interview active offenders. Had certain opportunities presented themselves, I would not have turned down such meetings. In fact, I have strong suspicions that in certain instances I was interviewing active offenders, who simply did not admit this fact. Usually members of the technology sector, these individuals instead talked in generalities and mentioned others they knew involved in various criminal activities, which they seemed to have an overly detailed knowledge of. What is accurate is that I aggressively pursued former cybercriminals in a way that I did not for active offenders, beyond a small number of enquiries, which went unanswered. These unsuccessful experiences pursuing active offenders helped shape my approach. Ultimately, I believed that this "former" group offered the most value for the limited time investment that I had available. Six years is a long time, but the scale of this project is immense, meaning that time pressures always remained. I made a strategic choice to focus on those who could be more easily located and who were more likely to agree to interview. I also had fewer doubts concerning the authenticity of their claims, as they had less fear of arrest than active offenders and could speak more openly, providing more detailed and reliable data. This meant I did not get caught in a quagmire of factually deficient interviews and seeking to verify numerous suspicious claims.

This last point is worthy of further discussion, given that there is a strong social science tradition of interviewing active offenders, some violent. Classics like William Foote Whyte's (1943) *Street Corner Society* pioneered the involvement of active offenders as study participants. A number of later exponents followed (see, for instance, Sanchez-Jankowski 1991, Murphy and Venkatesh 2006, Zhang 2008,

Goffman 2014). Some of these studies illustrate certain challenges involved in these approaches, but it is a generally accepted form of research for criminal populations. Why might the case of cybercrime challenge this tradition? The key difference is that many traditional offenders operate in the relative open. For cybercriminals, shielding their true identities is an essential part of doing business. Many operate in much more secretive ways than conventional criminals. Operational security aside, their crimes are also virtually invisible. This is what makes them more difficult to locate in the physical world and, when they are found, less likely to be fully forthcoming about their activities. The higher the level of business minded offender, the more likely they will operate in a more guarded way, which includes not speaking openly (or at all) with interloping researchers. Another strategy would be to access active cybercriminals in online spaces. But as noted above, questions remain about both ethical access to certain groupings and verifying exactly who or what version (persona) of that person is being interviewed. Personas are another protection for often-paranoid cybercriminals to hide their true nature from those who may put them at risk.

A separate distinction between traditional criminological research and cybercrime studies is that the risks to the researcher are not the same. Violence might be a heightened concern with some conventional subjects, but with cybercriminals the real difference is that once you are in their world you cannot escape. An urban ethnographer can leave a certain neighbourhood and be unlikely to have physical threats follow them. But a cybercrime researcher potentially faces cyber threats that could follow them wherever they are in the world. As a result, one might show extra caution when considering engaging widely with active cybercriminals, as the risks of

a negative interaction may endure. This lack of conventional territoriality also makes it unclear whether certain subjects are under police investigation. Carrying out interviews with those under investigation may have adverse effects on both the researcher and the participant, such as the demand for the release of confidential data that has been collected. These secondary distinctions provided added reasons to focus on former cybercriminals, in the given project timeframe.

As for the latter two participant categories, I chose to speak to law enforcement agents as they also have a strong knowledge of cybercrime, having spent much time investigating online crime. Why the technology sector provides a good source of participants requires further explanation. Given the challenges of cyber law enforcement, hampered by both technical requirements for investigation and a transnational threat that can make arrests more difficult, a number of private sector companies and other organisations have evolved in part to fill the void. Some have a sole purpose of gathering intelligence on cybercriminals or carrying out forensic investigations, while others are large companies that have developed/acquired specific units to carry out these functions. Some organisations protect themselves with large in-house teams. Other companies are serviced by external security teams. A number of these security companies also partner with law enforcement agencies and assist them in their investigations. In some instances and contexts, they can take on a very large responsibility for this. As a result, those with law enforcement-like experience in the private sector also became a valuable group within the project's sample.

Most participants were contacted directly or indirectly through online searches. In the early days of the project, I often identified law enforcement agencies and companies

that I believed would be relevant and then made contact through their publicly listed channels. In some cases this was surprisingly successful, with very helpful public relations officers finding me an appropriate participant to speak with. But in many more cases this strategy did not succeed: it either failed to elicit a response or the organisation declined to participate. In some cases where an interview was arranged by a company PR officer, there appeared to be certain expectations that it would benefit the organisation in a specific way. This might fit with some journalism, but it does not sit comfortably with academic research for either side.

As a result, I shifted my strategy to target individuals and attempted to contact them directly. There is now an extensive amount of personal information that is available online. This can be harnessed to find and profile potential interview subjects. For instance, many people provide a wealth of information on Linkedin (perhaps too much in personal security terms), even down to the specific responsibilities they carried out within a specific period and within a specific unit in their organisation. This type of social media also makes suggestions of other people with similar profiles, or who are connected to the profiles you have been looking at. This can be mined for information, leading to other possible participant names. Over time, I developed core profiles of the type of subject that would be suitable. For law enforcement this meant having experience investigating cybercrime. For the technology sector, it usually meant having experience in cyber intelligence or forensic investigation.

For former cybercriminals, along with public case records and media reports that could be used to identify possible participants outside prison, some former actors openly state their criminal background on their social media profiles or elsewhere. For

those who are not publicly known, there are other methods that suggest possible connections to cybercrime. For instance, those coming to cybercrime from a hacking perspective may list an involvement in the "security industry" from a young age, perhaps before they were likely to have been employed. Others might make note of their past hacking exploits. The profession perhaps most associated with hacking is what's known as a *penetration tester* or an *ethical hacker*. These are people hired by organisations to test their security. Some are trained for this through certifications, others have taught themselves to hack. Over the course of the project I found that some in this latter category had prior experience in cybercrime. This often made them useful participants. Of course, very many also had not been involved in cybercrime themselves, but some were still familiar with the world and may have known others who had been involved.

Contact with all three central groups was primarily made through email. The introductory email would describe the background to the project and request an interview. A number of those contacted did not respond, but many did. Sometimes they responded immediately, but in many cases I would follow up at least one more time. Persistence appeared to pay, as there were many instances where people agreed to an interview on the second contact. Perhaps they were busy or forgot, or perhaps the second contact signalled a more genuine and specific interest in meeting them. For subjects I considered very important, I would sometimes make contact for a third time if I had not heard from them, which led to occasional success. If someone declined at any point, I would of course bother them no further.

In the simplest cases, contact details were publicly available. In the more difficult cases, other email addresses for the organisation were available online or otherwise in my possession and the template could be used to determine the target's own email address. In the most difficult cases, no such template would be known and I would have to guess the template through trial and error, often leading to multiple bounces. In cases where I couldn't determine someone's contact details at all, I would sometimes seek to contact them through social media profiles like Linkedin, but this was only occasionally successful in leading to an interview. Finding contact details was sometimes as time consuming as choosing the most appropriate profiles in the first instance.

Cybercriminals can be difficult to locate and it is important to avoid studying only the low hanging fruit that can be more easily accessed. Approaching those in the manner discussed above, often led to a slightly skewed sample. I did manage to speak with cybercriminals of all levels, from those simply flirting with it to well known veterans of the industry. I also managed to cover a range from the very technical to those more centred on the money side. But the sample tended to skew more towards the technical and often, though not always to those who had subsequently found gainful employment in the technology sector. With some notable exceptions, the sample also skewed towards medium and lower level offenders.

As a result, I undertook one further activity to improve the sample's quality: interviews with prison inmates. A number of elite cybercriminals are held in prisons around the world, and potentially provide a very useful sample. This also helps overcome the problem of dealing partly with self-identified cybercriminals whose

veracity might be questioned. While I did not have strong doubts about the bona fides of those I spoke to and a number did have criminal records but had been subsequently released, this potential bias remains a concern for some (see Dupont 2014). Doing a small amount of prison research was very valuable in increasing the number of high-level cybercriminals in the sample. It also allowed for some more interviews with those primarily on the money side rather than the technical side, who tend to be more difficult to access in the outside world.

My initial intention was to conduct in-person interviews with inmates. But it soon became clear that this would not be practical. Accessing prisons for research has become an increasingly difficult and time-consuming process. Furthermore, cybercriminals are incarcerated in a range of prisons, sometimes in locations far from major cities, which increases the amount of time required, along with the financial resources. Prisoners are also moved and one could face the situation of travelling to a remote location and finding that the prisoner is no longer available.

Instead, I made use of email/mail interviews with a number of prisoners. I drew inspiration from prison researchers who had engaged in research by letter (see, for instance, Bosworth et al. 2005). In this case, the approach differed in that I wasn't attempting to study the broader prison population, but specific cybercriminals who happened to be in prison. Rather than advertising my project to different communities and hoping for responses, I drew up a list of desired participants and then contacted them directly. The lists were largely drawn from known cases and media reports. Those in the US prison system proved far simpler to access than those in the UK system, as there is a public website that provides information on whether someone is

incarcerated and where they are held. In the UK privacy restrictions prevent such a system and make locating inmates far more difficult and time consuming. The US also holds some of the most elite cybercriminals from across the world, due to the active role that US law enforcement plays in this area. I did not attempt to access prisoners in other jurisdictions. This was largely due to practical considerations in terms of limited time and resources, and difficulties in accessing inmates in some countries. But, as will be discussed below, there were also ethical considerations in terms of engaging inmates in some locations where their mistreatment may be more likely.

Once the location of a prisoner was determined, I would send them a letter outlining the study. Those who were interested could communicate with me by phone, letter or through a closed communication system available to prisoners that approximates email but does not allow general access to the Internet. This email system proved the most popular and effective form of communication. Phone was the least popular. Prisoners have a considerable amount of time on their hands and several participants engaged in extensive communications with me, going into details that one would not have time to broach in an in-person interview. While this form of communication did not allow me to read body language or assess other cues, I believed the richness of the data more than made up for this. Any misunderstandings through lack of tone or otherwise could be clarified in later communications. This method presents a number of advantages, not least cutting out time, cost, access issues, along with increasing standardisation across interviews and no requirement for subsequent transcription.

Some others communicated with me through letter, usually because they were not authorised to use the communication system. This approach provided some useful information but communications were generally shorter, due to the need for handwriting or using a typewriter, and there were much longer delays between letters. On the reverse side, detailed emails sometimes came more regularly than I could easily respond to them. This made it more difficult to build up a rapport and trusting relationship. It also made it more difficult to delve as deeply into details. Nonetheless such letters from elite cybercriminals can still provide gems that cannot be accessed elsewhere. Communicating by phone did not raise specific issues, other than scheduling complications as inmates have to call out, rather than the researcher calling in. Overall, I do not specifically list the number of inmates to whom I spoke as part of this study, nor the specific methods of communication. This ties to ethical issues that will be discussed below and the importance of providing as little contextual information on inmates as possible, which might somehow aid in identifying particular individuals.

Snowball Sampling

While purposive sampling was the primary approach used in this project, snowball sampling supplemented this where possible (on snowball sampling see Ritchie, Lewis, and Elam 2003, Hoyle, Harris, and Judd 2002, pp. 188-189). Snowballing was more difficult than has been the case with a number of other qualitative studies, where it is commonly used. Because the study engaged three core participant samples across a number of different jurisdictions, snowballing was always going to face challenges. Rather than one large snowball, a number of smaller snowballs by country or by

category was more likely. In some sense, the process is begun anew each time a new country is visited. But even this type of focussed snowballing proved difficult. This may be because the world of cybersecurity happens to be filled with a number of paranoid people, both on the criminal and enforcement sides. In a number of instances where interview subjects offered to connect me with other possible participants, an interview failed to eventuate. When the meetings did eventuate, it did not necessarily snowball any further.

Nonetheless, snowball sampling was still achieved in a number of instances and proved a valuable way to access certain participants. Referrals from existing participants helped provide access to subjects whom I may not have located on my own. Such referrals have broadened the sample. These referrals also generally led to a higher level of participation than through direct, cold, contact. In a number of instances, referrals led to interviews taking place when the participant had previously failed to respond to my unsolicited contact. Obviously issues of trust applied to myself, as much as they do to this study. Referrals are a very effective method in conducting this type of research, especially when the referee is well respected. In this way, snowball sampling corrected some of the possible deficiencies of purposive sampling and certainly added many valuable interview subjects to the sample, who could not be accessed through other means.

As would be expected, snowballing was most difficult in the early days of the project but improved over time. By the end of the project, I had built an extensive list of contacts across many countries and professions. Among these were certain individuals who acted as what might be called *global gatekeepers*. Given the transnational nature

of cybercrime and its enforcement, certain international networks have formed often among leading players. Each time I visited a new location, I would contact one or more of the gatekeepers that I suspected had the deepest contacts in the relevant region. This would usually lead to one or more suggestions of good interview subjects. In a number of cases, these suggested contacts came to act as local gatekeepers and often introduced me to further participants. In other instances, this role was sometimes performed by particularly helpful participants that I had contacted unsolicited. Sometimes even those who didn't meet with me served this role, offering what they believed were more appropriate suggestions in lieu of their participation if they were unavailable or unsuited.

Accuracy and Limitations

Over the course of the study, around 750 individuals (and organisations) were contacted. While there was some variation between countries, generally between 25-30% agreed to be interviewed. Another 25-30% responded to my enquiry but did not meet for the interview, either because they declined or it did not eventuate for some reason. The remainder did not respond at all. As with most qualitative studies, there may be some non-response bias in the sample. But the nature of this is very challenging to determine. Factors in non-response might include: apprehension of communicating with a stranger; a lack of confidence in their knowledge; a lack of confidence in their language ability; being overly busy; forgetting to respond; travelling during the interview period. In contrast factors in successful response might include: a strong interest in academic research and/or the world of cybercrime; an altruistic personality or cultural norms that encourage "hosting" visitors; an

international outlook or desire to meet a (foreign) visitor; boredom or free time during the work day.

The preceding sections have included some discussions of possible flaws and limitations in the data. This is always the case with qualitative studies, which often make use of non-random samples. But in many instances measures were taken to counteract the impact of these challenges, which are also incorporated into the discussion above. These measures would often fall under the key concept of triangulation (Patton 2002, p. 556, Denzin 1978). The central idea is that multiple data sources and perspectives can be brought together to limit the weaknesses within any specific source. This was achieved through many means in the study. First, the project draws on data from three groupings of participants. Each group has its own perspectives and its own possible weaknesses as informants. For instance, some might worry about those in the technology sector emphasising the threat of cybercrime as a business strategy. Others might be concerned that law enforcement would emphasise their own success in counteracting cybercrime. Others still might be concerned about former cybercriminals hiding certain sensitive pieces of information about their past actions. All these and more are genuine concerns, but are lessened by having all the interview categories combined, which provides internal checks and increases accuracy. Second, the study also draws on other forms of data that can be compared to the interview results, including legal records and cybercriminal communications. Unless there is an elaborate feedback mechanism occurring, multiple independent forms of data pointing to the same conclusion suggest higher levels of accuracy.

In some sense, one need not wait until all data is collected to triangulate. It is also important to ensure that each interview is as accurate as possible while carrying it out. The skill of the interviewer plays a significant role in qualitative research (Kvale 1996, Rubin and Rubin 1995, Marshall and Rossman 1999). Through good interview technique, information can be tested against other already collected data or other information already provided within that same interview. It is important to begin the interview with broad open questions, which allow the participants to answer without the interviewer prompting them and avoid pushing them towards specific responses that they might otherwise not provide. But once these responses have been given and the interviewer can ascertain the participant's unvarnished views, more direct follow-up questions can be asked if necessary.

These questions can be more closed or simply more specific. Their purpose is to verify or expand aspects of the account that has been given. If something that has been said conflicts with what is known from existing data, the relevant topic can be raised more directly. If the subject continues to display good confidence in the account, it is at least clear they believe it with certainty. This means that the area might require further investigation to harmonise or otherwise resolve the conflicting data points. If the participant quickly backtracks from a point when questioned directly on it, then one knows to view it with caution when compared to other data and may also seek to investigate the matter further. Existing literature delves into aspects related to this preceding paragraph, along with further detail on carrying out effective interviews (see, for instance, Legard, Keegan, and Ward 2003, 148-165).

Such checks on accuracy need not only occur externally, but can also be done internally. For instance, the background of the participant in question and the certainty with which someone speaks can influence how the responses are interpreted. If a law enforcement agent from country X makes a confident statement about cybercrime in that country, it is likely of higher value than a statement made by someone with no connection to X whatsoever, who seems uncertain about the topic, but wishes to offer an opinion on it nonetheless. One can also flag seemingly contradictory statements that are made within the same interview. These are very important to clarify if possible. If the subject can effectively resolve the apparent contradiction, then the data is more likely to be credible. If they cannot, then it should be used with caution. In some instances, a participant's general account may appear credible but may not connect closely with the central interests of the study and a more direct prompt may be required to gain their insights on these topics.

In terms of carrying out interviews, providing anonymity to participants was vital to the overall accuracy of this study. Anonymous reporting will be discussed again below in terms of ethics, but it had a number of practical advantages as well. First, it improved access to interview subjects and expanded the sample. A number of participants directly and indirectly indicated that they would not have participated without this assurance. These were often, though not always, those with strong knowledge of the subject and included law enforcement agents and former cybercriminals. Yet there were others in these categories who indicated that anonymity was not a major concern for them. Second, providing anonymity also likely improved the openness with which people participated and the amount of information that they offered. A number of participants suggested that they could

provide information that they otherwise would not be able to talk about if it were tied back to either themselves or their organisation. For instance, in one case I became aware that one of my subjects was a former cybercriminal only during the course of the interview and solely because anonymity was provided. Part way through answering my questions, he double-checked: "This is anonymous. Right?" and then proceeded to outline his past criminal endeavours in some detail, which remains some of the most useful data I collected over the course of the project.

Third, and linked to this previous point, I believe that the anonymity offered not only expanded the sample, but also improved the quality of the information. The way I could assess this was through a proportion of the sample that had previously given media interviews, which was sometimes how I had located them in the first instance. In some cases, the information they gave to me differed from their on the record interviews, but in ways that initially appeared counterintuitive. Despite having their name against the quote, the public record information appeared less accurate. Although it's unclear what role journalists might have played in this, sometimes this would be due to hyperbole such as overstating the threat of cybercrime or the involvement of organised crime groups. In other instances, these exaggerations were intended to demonstrate the effectiveness of their organisation or company in fighting cybercrime, such as by hiring cybercriminals to provide an inside perspective.

In terms of former cybercriminals themselves who went on the record, some played up their past criminality and some played it down. Those who highlighted their past deeds often did so as a form of promotion perhaps to secure or improve their place in the security industry. But for others, there were clear attempts to sanitise their past

deeds and downplay particularly destructive acts, their motivations at the time or aspects of their personal lives that might not encourage people to work with them as they sought to build new lives. When participants came to speak to me on the provision of anonymity, a number pulled back from their on the record statements, and often offered far more measured accounts. Part of this may also have been due to this being an academic project, which seemed to push some participants to view accuracy as being a much more important issue than with regard to journalism. Ultimately, I believe that providing anonymity for all participants reduced the potential for them to promote other agendas and improved overall accuracy.

The large amount of data that is drawn on for this study also helps matters in terms of accuracy. While a case study may provide rich data, it may not be very generalisable. The broad approach taken in this project draws on many cases and many jurisdictions, greatly increasing its external validity (Hoyle, Harris, and Judd 2002, pp.32-33, 41-42). The extensive variation within the sample is also helpful in avoiding selection on the dependent variable (see King, Keohane, and Verba 1994, pp. 129-137). If one wishes to study the presence of a phenomenon (the dependent variable) – in this case cybercriminal cooperation – one should also examine instances where that phenomenon is absent – failures of cooperation. Otherwise one might fail to determine which independent variables are necessary for the presence of the phenomenon under study, and which are present regardless of whether that phenomenon occurs or not. In this study, this variation was provided in a number of ways: 1) through examining cases over time through periods where cybercriminal cooperation was successful and others where it was less so; 2) geographical variation also meant that some countries saw high levels of cooperation among their local

cybercriminals, while others saw such cooperation hindered; 3) the accounts of the cybercriminals themselves also provided micro-level instances of where they succeeded at cooperating and where they failed.

Ultimately, despite these measures, there will always remain some biases and limitations. This is the case with all research, but there are particular challenges that relate specifically to qualitative research. While little can be done to address such concerns, it is important to acknowledge these biases and limitations and factor this into the overall anaylsis. First, all interview data faces similar concerns over credibility. It is possible that interview subjects may provide misinformation intentionally or accidentally, they may hide aspects of their account or they may forget certain details over time. For instance, companies may play up the threat of cybercrime, while law enforcement from a specific country may downplay it to present a rosy picture to outsiders. The measures described above, such as triangulation, reduce such risks but some will always remain. Second, the sample of participants along with the other data that is used is not random. While scientific inference can still be applied to such a sample, it is difficult to generalise the findings in a concrete way. Instead the results of studies like this one offer more suggestive findings and outcomes. Ritchie, Lewis, and Elam (2003, p. 78) explain such sampling in this way: “The sample is not intended to be statistically representative: the chances of selection for each element are unknown but, instead, the characteristics of the population are used as the basis of selection. It is this feature that makes them well suited to small-scale, in-depth studies”.

There are also points specific to this study that should be acknowledged. It is possible that the sample does not include certain key participants who might alter the nature of the results. The nature of law enforcement and private sector involvement in the cybercrime sphere is possible to delineate and I am fairly certain this study includes a reflective cross section of these groups and the range of participants in them. For cybercriminals this is more difficult largely due to issues of access. While I also believe I have a good cross section of cybercriminals across countries, areas of specialisation and ranging from low level to high level offenders, there remains at least some doubt that certain key participants might be missing from the sample. First, for the reasons described above, only former cybercriminals are included in the sample. There may be something qualitatively different between former cybercriminals and those who remain in the business. Active cybercriminals have not been arrested yet, or again, nor have they chosen to retire. Some information is provided on this group by the former cybercriminals who dealt with them, but they are not heard from directly in this study. This is a possible bias that must be acknowledged but cannot be directly counteracted.

It is not entirely clear what the impact of this data hole is on the accuracy of the study. There might be little difference between the two cybercriminal categories, if it's simply a matter of time before various active cybercriminals become former ones. Or, it is possible that the two samples are quite different. For instance, those that voluntarily retire from cybercrime might be less committed to the business and have other opportunities they can turn to than those who remain involved. A different concern in traditional criminological studies, is that arrested offender populations might over-represent low-level street offenders, as these people make easy targets for

arrest. This skew would mean that the higher-level actors would not be represented in the sample. But in cybercrime, the situation appears to be different. There are simply too many cases for law enforcement agencies to investigate. While some small fish are arrested, in many cases the policing strategy appears to be taking out high value and high profile targets, maximising the impact of minimal resources, perhaps as part of a strategy of deterrence. If anything, this means those that are arrested could skew to the higher echelons of cybercrime – those worth arresting – rather than the small timers.

If there is a segment of cybercriminals missing from the sample, it is most likely those who are extremely cautious. It is those actors who raise their heads too high that appear to get caught. The "smart ones" avoid high profile targets that are likely to attract the full force of a law enforcement agency, even if that means a lower payoff. They would also be more careful in their personal lives, not going on holidays to locations where they may be arrested and extradited, as is somewhat common among international cybercriminals. They would probably also not participate in an academic research project and give information on their criminal dealings. They may not make the most money in the industry, but if these ghosts exist, they are likely missing from this, sample beyond what others say about them.

Ethics

This project made use of standard ethical protocols for carrying out qualitative research and interviews in particular. Gaining informed consent is the foundation of such studies (see Israel and Hay 2006, ch 5). In order to gain their consent, I

explained the nature of the study to all subjects. According to my university ethics clearance, it was standard procedure to present each interview participant in this project with a form that also outlined the key aspects of the study. Many participants consented in writing. A substantial number consented orally instead. In countries where signed documents are viewed with suspicion, oral consent was common. But it was also a personal decision regardless of context, with some preferring not to have an official paper trail linked to them.

Given the sensitivity of some of the topics and participants involved in this study, anonymity and confidentiality were also fundamental. All the names of participants in this study have been replaced with pseudonyms. I have also attempted to list only in the appendix the most essential information about subjects. For instance, I do not identify specific law enforcement agencies in each country. The world of cybercrime is still a relatively small one, for offenders and enforcers alike, and some seemingly innocuous details can have a bearing on revealing possible identities. There is a small number of participants who reside in a country that differs from their nationality. In certain cases this may disclose their identity, if for instance they are one of few people of that nationality working in the security sector in the country. In such cases I have included them in their nationality category, particularly if the information they provided relates largely to that context. If the information they provide does not primarily relate to their national context, I list them more broadly as an *expatriate* of no stated nationality residing in the relevant country. For similar reasons, I provide only the year of each meeting to avoid clear references to specific conferences where someone might have been interviewed and attendee lists might be accessed.

With regard to the former cybercriminal participants, I took the further step of identifying them only by region rather than by country/nationality. This is due to the extra sensitivity involved with these participants and the small pool of known offenders of whom some are included in this study. For similar reasons, I also do not differentiate between those who are currently in prison and those who are not. In rare cases, I may make mention of arrest in the text if it is essential to the point being made, but I try to avoid too much detail on time served and related issues that might be used to narrow down the case. In certain cases, I interviewed members of the IT sector in various countries that I suspected may have had past or ongoing involvement in cybercriminal activities. Unless these participants actively acknowledged their involvement, I do not report these suspicions. Without providing such sensitive information, I therefore include them in the general lists of interview subjects, rather than the list of former cybercriminals. Israel and Hay (2006, pp. 82-85) provide a useful overview of similar precautions that have been carried out by scholars in other studies.

Along with employing pseudonyms, I also make use of a code to identify each participant. The first part of each code lists the country where the participant is based, or region in the case of former cybercriminals. The second part lists their profession. Where they have had multiple roles, I have listed the one that is most closely linked to the information they provided. In certain cases when it's relevant, I also note any secondary roles in text. The final part of each code is the number of that participant type in chronological order. For instance, UK-LE-3 means that the person is an active law enforcement agent based in the UK and that, chronologically, they were the third such person that I spoke with. Two complications are when someone is an expatriate

or they provide information largely derived from a former profession. To illustrate these more complex cases, here is another example: SEA(E)-(F)CC-1. This is the code for an expatriate based in Southeast Asia, who is a former cybercriminal, and the first of that type whom I met. The country and regional signifiers should be relatively intuitive but are also contained in the appendix headings. The tables below summarise the profession and country/region signifiers that are used:

Table 1: Profession Codes

Code	Meaning
A	Academic
CC	Cybercriminal
CSP	Cybersecurity Professional
FSP	Financial Sector Professional
H	Hacker
ITP	IT Professional
J	Journalist
LE	Law Enforcement Agent
OO	International Organisation Officer
P	Prosecutor
(F)	Former

Table 2: Country Codes

Code	Meaning	Code	Meaning
AUS	Australia	NIG	Nigeria
BRA	Brazil	ROM	Romania
CHN	China	RUS	Russia
EE	Eastern Europe	SEA	South East Asia
GER	Germany	SGP	Singapore
HK	Hong Kong	SWI	Switzerland
IND	India	THA	Thailand
INT	International	UDL	Undisclosed
IRE	Ireland	UK	United Kingdom
LAT	Latvia	UKR	Ukraine
MY	Malaysia	US	United States
NA	North America	WE	Western Europe
NLD	Netherlands		
(E)	Expatriate		

All direct quotes from these participants are verbatim, or as close as transcription allowed. In the case of written interviews, responses are reported without editing for grammar or spelling.

For the most part this study did not engage with subjects from particularly vulnerable populations. No subject was under the age of 18 or suffering from known mental disabilities. Former cybercriminals are likely the most at risk, but the risk is still somewhat low, given that any criminal behaviour was in the past and often known by others or with some degree of public record. There is also no shortage of cybercrime cases for law enforcement to pursue, leaving little interest to compel a researcher such as myself to divulge information on past offenders, and which I would have refused to do. In fact, I interviewed a large number of law enforcement agents who were aware that I was also interviewing former cybercriminals. No such requests were made or even suggested, with most participants across all groups being aware of the importance of independent academic research. This appears to differ from some other forms of crime, where researchers have faced unwanted interest from law enforcement agents and others (Israel and Hay 2006, pp. 85-90, Jacobs 2006, p. 158).

Nonetheless, there was one class of former cybercriminals in a more vulnerable position: prison inmates. I address the ethical means with which I approached this group in the subsections below.

Inmates and Ethics

Doing research with prisoners presents a number of ethical considerations. Nonetheless, if a researcher applies the correct measures, these issues can be overcome. In fact, criminologists and others have undertaken a number of successful prison-based studies, which have made use of many more prison interviews than this thesis (see, among others, Morris, Morris, and Barer 1963, Genders and Player 1995, Sykes 1958). At present, the British Society of Criminology Code of Ethics (the Code), the most relevant protocol of its kind for this project, provides only limited guidance for conducting research with prisoners.[11] While making use of the elements of the code that do apply, along with an application of its general principles, I also examined the relevant literature in this area, which provides the most direct guidance on ethical issues in this field of research (Bosworth et al. 2005, Matfin 2011, King 2000, Liebling 1999, Sorensen 1950, Giallombardo 1966).

Below I outline the key concerns that I needed to be aware of in conducting this research and the appropriate measures that I undertook. In most cases, these issues related to gaining informed consent in these special circumstances. As I did not physically visit the prisons, consent was attained through writing. Given the vulnerable nature of prisoners, it did not seem appropriate to require a signed consent form from them, especially when not presenting it in person. Many outside prison are already intimidated by signing what looks to them to be a formal binding document (even though such a form largely spells out the protections they will receive).

[11] The latest version of the British Society of Criminology's Code of Ethics can be found here: http://www.britsoccrim.org/documents/BSCEthics2015.pdf. There are also other codes with a more medical focus that I have consulted, but are not directly relevant to social science research. See for instance: http://www.hhs.gov/ohrp/policy/prisoner.html.

Prisoners would also have to mail the form back to me, thereby accruing (unnecessary/international) postage costs. As a result, the standard approach I adopted was to present the information contained on the consent form as key points the prisoner participants needed to understand. For those communicating by letter, this information was in a document without a space for a signature. For those communicating electronically, I cut and pasted the same information into a message that I sent them. Rather than require them to sign anything, I specified that they should read the material and let me know if they had any questions. We would only proceed with the interview once they were satisfied and felt comfortable. Some seemed to have few concerns with the nature of the study; others engaged in a long back and forth with me about different aspects of how the information would be used. After this discussion had addressed their concerns, or various limitations on their participation had been stated, they would then indicate they were happy to proceed.

Incriminating Admissions

During interviews, inmates may provide information on crimes that have not been the subject of legal proceedings. This could put both the researcher and the participant in a difficult situation. The Code explains this issue by way of a "frequently asked question":

> Q1: "One of my interviewees in prison has told me about getting away with various offences. He told me he is in prison for three burglaries, but there are several other offences that the police don't know about. What should I do?"
> A1: It should have been made clear to participants in the research at the outset what the limits of confidentiality for those involved in the study were: see sections 4iii and 4iv of the Code

> of Ethics. Research in sensitive settings such as prisons is particularly likely to throw up issues of this kind.

The relevant parts of the mentioned sections to be applied are:

> 4(iii) Research participants should be informed about how far they will be afforded anonymity and confidentiality. Researchers should pay special attention to these matters when participation is sought from children, young, or vulnerable people…
>
> 4(iv) Offers of confidentiality may sometimes be overridden by law: researchers should therefore consider the circumstances in which they might be required to divulge information to legal or other authorities, and make such circumstances clear to participants when seeking their informed consent…

Bearing these sections in mind, I adopted the approach of offering inmates complete confidentiality and a promise to report data anonymously, changing participants' names and key details that could be used to identify them.[12] But I was aware of the issues raised above, the potential complications involved and the risks I was taking on. As a result, I specified to inmates that they should only answer questions with regard to crimes for which they had been tried/convicted. I indicated the importance of steering away from sensitive topics to avoid potential legal issues for both the inmate and myself. While it is beyond the focus of the project, I also specified that the interview should not cover behaviour inside the relevant prison, to avoid knowledge of potentially sensitive information in this regard, which a researcher might feel some compulsion to disclose. The tension between maintaining confidentiality and knowledge of purported information about a prison break or internal assaults is a

[12] In general, there is no legal obligation for researchers to reveal undisclosed criminal actions to law enforcement unless compelled by them to do so. The statute covering this is the Criminal Law Act 1967 s.4 and s.5.

difficult one. This is generally regarded as a complex grey area, and it is ultimately up to the researcher to best decide what action to take in the specific circumstances (Matfin 2011, p. 229, Newman 1958). But this issue did not arise in the course of my fieldwork.

Informed Consent and Potential Coercion

In terms of the Code and the discussion above, informed consent is a vital requirement of participant based research. In the case of prisoners, issues of potential coercion can complicate this process. Matfin outlines the problem:

> Despite public perception to the contrary, prisoners are an extremely vulnerable group of people, without the freedom to walk away from a situation or the normal recourse to legal help and advice. They cannot pick up the telephone at will or pop into a friend's house to discuss what they should do. They may feel that to co-operate might be detrimental to their position but that not to co-operate could have even worse consequences for them. They are a powerless group of people about whose lives others take all the decisions, whether they like those decisions or not (Matfin 2011, p. 221).

The most important measure to take in this regard is to be aware of the vulnerability of prisoners and to be extremely careful in gaining informed consent. With all participants, I took care to explain the research fully: both what they were participating in and potential implications. But in the case of prisoners, the *voluntary* nature of participation was also stressed. As I dealt directly with prisoners and did not require a prison officer as an intermediary, this reduced the potential for accidental coercion. Consent was gained directly from each inmate and we often engaged in several back and forth communications before beginning, to make sure that

everything was understood and the inmate was satisfied with how matters would proceed.

With all this said, I believe that inmates generally viewed their participation in this study as a positive experience. The rapid fire and detailed responses I received from some indicated that this activity was something they were happy to spend considerable time on. Carrying out research by mail, Bosworth et al. (2005, pp. 254, 256) find something similar: the prisoners enjoyed participating in projects because it gave them something to do, engaged their minds, was an opportunity to express themselves and potentially make a difference, and/or allowed broader social contact. As Matkin puts it:

> One distinct advantage of carrying out research among such a literally captive audience is that the refusal rate is usually low. Prison is an excruciatingly boring place and the boredom often makes prisoners willing to participate. Once the research has been explained to the inmates and staff, and if the prisoner understands that s/he *need* not comply with the request for an interview, then consent to participate is very much dependent on the individual skills that the researcher needs to employ. Can the researcher offer *anything* the prisoner wants? It is very unlikely that the inmate will agree to an interview if the answer is no. Prisoners agree to be interviewed because they will get something out of it for themselves. This is known as the *research bargain.* Whilst no inducements may be offered, that does not mean the prisoner does not weigh up whether there is likely to be any other advantage attached to the interview. For the researcher, working out exactly what that advantage might be can be complex, but it is the key to why inmates agree to be interviewed and then often reveal deeply private information. In some circumstances, the bargain may be as straightforward as the prisoner simply wanting to talk to someone different about almost anything other than their immediate surroundings (Matfin 2011, p. 228).

For the inmates included in this thesis, I believe the subject matter was particularly important to them. A number of former cybercriminals I interviewed across this study had a passion for technology and cybersecurity beyond their criminal endeavours. Sometimes they would indicate to me that they enjoyed speaking with me about the issues I was studying and might also ask me questions on the topic following the conclusion of the interview. For inmates, the pool of people they can speak to about these issues can be limited. One prisoner interviewed in the study indicated that he enjoyed our communications because he had no one else at his facility who understood anything about the subject. Another possible motivation was that some enjoyed sharing their expertise and being acknowledged for their abilities, while also seeing their views making research more accurate on the subject of cybercrime. While inmates may have felt they benefitted by participating in the research, I did also make clear to inmates that participation carried no specific rewards, nor any disadvantages (Matfin 2011, p. 221).

Weakened Anonymity and Confidentiality

While confidentiality and anonymity were offered to every subject in this study, it is important to note that communications with those in prison may be monitored by prison officials. Despite offering full confidentiality and anonymity on my part, I also had to make this possible surveillance clear to each inmate at the outset. At various points, particularly when some subjects started to get carried away, it was important to remind them of this point. But in other instances, certain inmates appeared to be very aware that their communications were being monitored and would self-censor. For instance, they would not use the names of former collaborators who had not been

arrested or would indicate to me that they had removed certain details from an account that might be sensitive.

Conclusion

This chapter has outlined central issues relating to data and methods in this thesis. The first section addressed the research style; the second section outlined the data and its collection; the third section discussed the study's scope, sampling and limitations; the final section addressed key ethical considerations. With this background covered, the following chapters begin the substantive portion of the thesis with its central focus on the industrialisation of cybercrime. The next chapter opens this discussion with an account of the history of cybercrime.

3. The Evolution of Profit-Driven Cybercrime: From Lone Wolves to Industrialisation

This chapter provides a history of profit-driven cybercrime. It charts the evolution of financially motivated cybercrime from its origins to the present day. This has seen a move out of activity that was largely informal, focussed on recreational and ideological concerns, and was often not illegal in the early days of hacking, to the present where cybercrime has grown to incorporate a large, illicit and somewhat professional industry, heavily driven by profit. It is largely a story of a shift from lone wolves to industrialisation.

There is surprisingly little literature on the development of cybercrime. Some of the major social science texts on cybercrime provide scant background on this point (Wall 2007, Yar 2013). While the history of hacking in the West has received some attention from academia, journalism and elsewhere, the focus has been largely on hacking rather than cybercrime specifically (Levy 2010, Dreyfus and Assange 2012). Even those directly addressing cybercrime often focus broadly on the development of hacking, malware and related activities, and give only secondary attention to profit-driven enterprises (Brenner 2010, ch 2). Such works have also tended to focus on the US and other parts of the West, giving little thought to those countries that are now the engine of the cybercrime industry, such as those in Eastern Europe. They have also often centred on the time period from the late 1950s to the turn of the millennium, tailing off at the very point at which profit-driven cybercrime began to flower. There is a small number of journalistic accounts, which provide potted histories of aspects of this more commercial form of cybercrime (Glenny 2011,

Poulsen 2011, Menn 2010, Krebs 2014). Though useful, these historical accounts are often truncated, as the focus of such popular books is on the specific stories they are telling rather than a more comprehensive exploration of the evolution of financially motivated cybercrime.

While it addresses the limited existing accounts, much of this chapter has to be drawn from other sources. Legal documents, whether publicly available or furnished to me directly, afford one useful avenue for relevant information. But in many cases a number of documents that would provide fertile ground for research are sensitive and understandably held close by the relevant government agencies. This is not to mention that such documents would not have recorded every aspect of cybercriminal business, some of which remains even out of law enforcement reach. There are also various digital footprints that have been archived and/or published, such as elements of now defunct forums that played an important role in their day. Some cybercriminals have also made public statements about certain issues. These all provide important clues in tracing the evolution of profit-driven cybercrime. But on their own, they are not enough to provide a rounded picture of how profit-driven cybercrime has developed. As a result, a significant part of this chapter is an oral history of cybercrime, drawn from interviews with those who directly participated in events and those who tracked them.

This chapter contains six main sections. The first section outlines a brief history of hacking, beginning with the early days when hacking did not involve illegality. The second section addresses the turn to illicit profit-making activities in the 1990s, while the third section recounts the rise of online cybercriminal trading forums and their

Golden Age. The fourth section examines the specialisation of forums that took place, while also addressing the fragmentation of the market that followed the end of the Golden Age. The fifth section is focussed on the development of operational structures and groupings that carry out cybercriminal activities, while the sixth section provides an account of the growth of essential cybercriminal "infrastructure" like virtual currencies and bulletproof hosting. The final section briefly assesses the current state of cybercrime and cybercriminals.

A Brief History of Hacking

While some locate the origins of hacking back through human history, computer hacking by definition is a much more recent phenomenon. Its origins are conventionally traced to MIT in the late 1950s (Levy 2010, ch 1). The first hackers were students at MIT, driven by intellectual curiosity, who began to experiment with the university's mainframes, the prototypical computers of the day. As Levy (2010, ch 2) recounts in his classic text *Hackers*, a "hacker ethic" soon emerged based on some foundational ideas that persist to varying degrees in the present day: that access to computers should be "unlimited and total"; "All information should be free"; authority should be mistrusted; "hackers should be judged by their hacking" rather than other characteristics. These core ideals were supplemented by some inspirational mantras: "You can create art and beauty on a computer" and "Computers can change your life for the better". This hacking culture soon spread to other university computing centres, which was further assisted by the development of ARPANET (Advanced Research Projects Agency Network) in the late 1960s, the first major network linking hundreds of universities, research institutes and companies (Yar

2013, p. 7, Brenner 2010, p. 15, Hafner and Lyon 2006). At this point, hacking did not involve any strong sense of maleficence, but was largely recreational and intellectual.

The other early activity often connected with computer hacking, but involving phone technology instead, was *phreaking*. This practice followed a similar timeline to early hacking but faded away with the introduction of digital phones. Nonetheless, it played an important role in the history of hacking and the individual narratives of some who would become very well known hackers, such as white hats like Steve Jobs and Steve Wozniak and black hats like Kevin Poulsen and Kevin Mitnick. *Phreaking* involved the manipulation of phone systems to make free calls by creating a 2600-Hz frequency tone through whistles or other means. While *phreakers* profited through free calls, exploration and research into this new frontier often appeared their main driver (Brenner 2010, pp. 13-14).

Beginning with the MIT hackers, and as the hacking community expanded more widely in following decades up to the 1980s, the tradition was largely about intellectual curiosity. This was also before the introduction of relevant legislation banning computer intrusions and other activities. One pioneer of hacking in Europe, who operated in the 1980s, explained his motivations in this way: "I was about twenty one, twenty two, hacking for fun, not to gain any money, never did. Purely for fun, challenge of breaking into machines. Never really made any secret of it". He described his activities as not being "anything desperately clever", but being possible because "people left passwords where they shouldn't have done" (WE-(F)H-1).

But during the 1980s, matters started to become more serious both in terms of the

hacking activities taking place and the responses to them with respect to increased legislation and enforcement. By this time, personal computers had become more widely available and computer systems were becoming increasingly networked and developing toward what would become the Internet. This provided a larger group of potential hackers, rather than just university students with access to the institutional machines, and a larger range of targets. Some hackers in this period displayed darker motivations, causing significant damage and capturing the attention of authorities. Perhaps the most famous black hats of the time were Kevin Poulsen and Kevin Mitnick. Poulsen began *phreaking* and hacking into ARPANET in the early 1980s, but later as a fugitive from the law (1989-1991), he turned his skills to rigging radio station calling in competitions to win cars and money (Littman 1993, 1997). Mitnick was involved in a number of serious intrusions against both government institutions and corporations, but profit never seemed his primary goal (Mitnick and Simon 2011, Brenner 2010, pp. 23-26).

At this point, a degree of organisation also began to emerge and hacking groups developed. Some of the most famous of these are the Chaos Computer Club in Germany, the Cult of the Dead Cow in Texas, as well as other former groups like Legion of Doom and the Masters of Deception. Such groups blended traditional hacker ethics, with its interest in information sharing and open boundaries, with what might be regarded as aspects of early hacktivism (Slatalla and Quittner 1995).[13] Some members also breached criminal codes in particular jurisdictions by intruding into systems and engaging in other activities. A number of members of Legion of Doom and Masters of Deception faced prosecution for a range of offenses. Meanwhile,

[13] See also http://cultdeadcow.com; http://www.ccc.de/en/.

hackers loosely affiliated with the Chaos Computer Club were caught penetrating US systems in the 1980s and selling the data to the KGB. Clifford Stoll's classic *The Cuckoo's Egg* recounts his personal hunt for one such hacker (Stoll 2007).

Development of malware (malicious software including viruses and worms) took a similar course to the evolution of hacking. In the 1980s, most viruses and worms were created out of intellectual curiosity or mischief. Perhaps the most famous example was the worm released in 1988 by Robert Morris, a graduate student at Cornell. The worm wreaked havoc on computer systems, but that did not seem to be Morris' motivation. Once he realised what was happening, he tried to notify others of how to stop the worm.[14] In the 1990s and early 2000s, malware became increasingly malicious and destructive, but the motivations still ostensibly centred on mischief and cyber equivalents of vandalism rather than on anything specifically profit focussed (Brenner 2010, pp. 30-36).

The Turn to Profit

The conventional history of hacking usually ends around the turn of the millennium. But it is at this point when the history of profit-driven cybercrime begins in earnest. One retired senior FBI official summarised the shift to the next phase of cybercrime:

> I think that it has evolved, I think that it has evolved to become organised. I think earlier on, it probably really starts where it can be measured in the late 90s. Before that the connectivity and the commerce was not robust enough for it to be anything really profitable. I mean there was hacking, there has been hacking since the 80s, but the infrastructure and commerce didn't really

[14] *US v. Morris*, 928 F. 2d 504, United States Court of Appeals, 2nd Circuit 1991.

> take worldwide until the late 90s. And I think early on in the late 90s, the type of crime that was committed was more the equivalent of vandalism: people were defacing websites, there were denial of service attacks, there was absolutely state sponsored intrusions back then, but not the level of criminal activity that we see now fast forward 12 years later, 15 years later, and you see because of the way our economy has evolved and the way organisations have pushed data to the network, the value of the data is so great, it's inevitable that this, that crime would migrate to the network because that's where the money has migrated (US-(F)LE-2).

Two things distinguish the history of profit-driven cybercrime from that of hacking. First, as noted in the introduction, cybercrime is not interchangeable with hacking. There are many aspects of cybercrime that do not involve hackers or hacking. While some aspects of the history of cybercrime derive from hackers shifting into criminal activities, there are also examples where that is not the case. On the other side, there are also many hackers who have no involvement at all in crime, and statements to the contrary can cause offence to this substantial subsection of society. Second, while the history of hacking has US roots, or rather is conventionally ascribed in such a way, the origins of profit-driven cybercrime are often found in other countries. In fact, in some ways it is more accurate to refer to multiple histories of cybercrime, with each geographical location producing its own brand of cybercrime. A number of these origin stories deserve considerable attention, but are too many to address comprehensively in the scope of this chapter and thesis. Some will be touched on in a later section and in the following chapter, but the general narrative remains similar in each case. From the 1990s onwards, computers and access to the Internet become more widely available for users across the globe, just at the time when increasing amounts of data and commerce are being digitised and finding their way online. All across the world, an economic opportunity emerges to tempt both the technologically

adept and those simply looking for new ways to make money.

In certain cases, a pattern emerges, with the development of local cybercrime taking place in phases. The first phase often involves students, among others who have access to new technologies, an eagerness to explore and time on their hands. At first, profit is not a major concern. This has been seen in examples as diverse as the United States, Russia and China. At some point a second phase and perhaps second generation emerges that is much more focussed on financial gain. These groups may abandon some of the ethics and even rules of the earlier generation (US-(F)LE-2, RUS-ITP-1, CHN(E)-CSP-1). Of course, this narrative does not always hold. For instance, in Romania and Nigeria where much cybercrime is less technical, the profit-imperative is apparent from the early days. But in such cases a shift towards greater "professionalism" and more serious earnings takes place over time (ROM-(F)LE-1, NIG-ITP-1, NIG-(F)LE-1).

The above discussion links to the importance of geographical context in understanding cybercrime, which will be tangentially addressed as part of the next chapter. As noted above, the scope of this chapter does not allow for a thorough examination of all the localised forms of cybercrime around the world. Instead, the remainder of this chapter is concerned with the development of the global market for cybercrime. In some ways, this online space has managed to bridge some of the different geographical concentrations of cybercriminals and allow them to conduct business together. It is ostensibly open to actors from any country around the world, so long as they have some value to add to the community. It has led to the development of a distinct, and flourishing, transnational cybercrime industry.

The Golden Age of Forums

The 1990s saw the birth of profit-driven cybercrime. Various financially motivated intrusions and scams came into existence. While a number of cases went unnoticed or unreported, some key investigations became emblematic of what was to come. In 1994, the St Petersburg based Vladimir Levin successfully penetrated Citibank in the United States, leading to the illicit transfer of over US$10 million through a well organised network of accomplices (FBI 2014). In 1997, Californian Carlos Salgado stole a large database of 100,000 credit card numbers and associated data by hacking into a major Internet company. Salgado attempted to sell the database for $260,000, but it was likely worth considerably more (The New York Times 1997).

As large as the potential damage was, the Salgado case is perhaps more important in illustrating the nature of financially motivated cybercrime during the 1990s. While individuals and small groups were starting to involve themselves in criminal activity online, there was very little organisation and no sense of the industry that would come. In his excellent book *Kingpin*, former black hat hacker turned journalist Kevin Poulsen, who was mentioned above, describes (somewhat derisively) how Salgado attempted to sell his wares online through the #carding IRC (Internet Relay Chat) chat room under the nickname SMAK:

> It was like offering a 747 for sale at a flea market. At the time, the online credit card fraud underground was a depressing bog of kids and small timers who'd barely advanced beyond the previous generation of fraudsters fishing receipt carbons from the Dumpsters behind the mall. Their typical deals were in the single digits, and their advice to one another was tainted by myth and idiocy. Much of the conversation unfolded in an open channel where anyone in law-enforcement can login and watch –

> the carders' only security was the fact that nobody would bother (Poulsen 2011, p. 38).

The turn of the millennium brought this period of disorganisation to a close. It was at this point that the true marketplaces for cybercrime began to emerge. In the early days, most trading between cybercriminals was done over IRC. Lance, a North American veteran of the carding scene and pioneer of the early forums, who has since left the business, explained the deficiencies involved with the IRC format:

> Before the forums, everything was done through IRC. The problem with IRC was it was so quick that people could come and just say anything and it was really hard to conduct business. So what the forum purpose served was that you could see these posts going on and you had a record to refer back on, as far as what these people were talking about. With IRC you didn't really have that. Once a conversation was done, it was done. So the forums allowed that history and for users to look back and say okay this guy has been talking about this this this and this. And to a point that allowed people to get a vibe for the seller or the buyer to see if they were able to do business, if they were able to trust them (NA-(F)CC-3).

The introduction of forums revolutionised the way business was done. It was the effective birth of the cybercrime market and the increasingly professional industry that followed behind. Cybercriminal forums are not dissimilar to Internet forums on any other topic. They are a series of *boards* that have different topic areas where discussion threads can be posted and other users can respond. As Lance explained, this format crystalised discussions and allowed them to be recorded for later viewing, rather than disappearing into the online ether. Over time, a number of other functions emerged that facilitated more effective business dealings, such as product review systems and the provision of escrow services. These elements will be addressed in

more detail in chapter 6.

The specific history of forums itself is a little murky. The Ukrainian forum CarderPlanet has taken on a central status in the cybercrime narrative (see Poulsen 2011, pp. 73-75, Glenny 2011, part II, Menn 2010, ch 9). But while its impact was probably the greatest in providing a model for the way future marketplaces would be run, it was not the first. That honour is shared by a range of forums that were either outright scam sites or others that were not very effective at their role. Lance described getting conned by a scam forum in the late 1990s where the administrator maintained multiple identities and posted positive reviews about himself back and forth (NA-(F)CC-3).

The first (known) genuine attempt to overcome these issues in English was a forum called Counterfeit Library. While Counterfeit Library came to address this need in the market, it was hardly a "cybercrime" forum in its genesis. It was founded by a small number of fraudsters based in North America in 2000, who were not highly technical operators. It began as a place to complain about being ripped off, but quickly evolved into a marketplace for the trade of fake documents, such as IDs, which are useful in conducting many types of fraud (NA-(F)CC-3). The key contribution that Counterfeit Library made was to provide a credible meeting place online for various types of fraudsters and other criminals, along with a mechanism by which they could establish a brand (Poulsen 2011, pp. 73-74). The nature of boards as opposed to IRC helped somewhat. But the site also offered a new innovation: in order to sell products on the forum, the products had to be reviewed by the administrator, by physically sending a copy to him (NA-(F)CC-3). Merchants had to be vetted. It was an early version of

what would later become common practice in many cybercrime forums: the verified vendor.

There is little doubt that Counterfeit Library predated CarderPlanet. But there were also some prototypical developments on the Russian speaking side of the cybercrime world. Script, the entrepreneurial Ukrainian cybercriminal who would go on to found CarderPlanet described seeing another earlier website, www.carder.org, which inspired his efforts. He believed that this existing site was the first on the topic of carding but had poor quality information. Script and his friends created a new website called www.carder.ru, intended to remedy the deficiencies. That site was shortlived, but it was followed by the creation of CarderPlanet, which would revolutionise profit-driven cybercrime (Xakep.ru 2002).

The origins of CarderPlanet have taken on somewhat mythical proportions because of evidence that the key players met in person and held a cybercrime "convention" in Odessa, Ukraine. But accounts differ on this point. Poulsen (2011, pp. 73-74) recounts a 2001 meeting where 150 Russian-speaking cybercriminals met for a summit in a restaurant in Odessa to discuss the launch of CarderPlanet. He suggests they were spurred on by the success of Counterfeit Library and that the conference attendees were eager to create a Russian language site that would allow them to congregate online and do business. A short time after the summit, the International Carders Alliance was established, along with the website called CarderPlanet. Meanwhile, in his book *DarkMarket*, Misha Glenny describes a meeting in Odessa taking place in 2002. This was The First Worldwide Carders' Conference, marking the anniversary of CarderPlanet's birth. He suggests that the main meeting was held in the Odessa Hotel,

with other smaller, more exclusive, gatherings taking place throughout the city. The meeting was not about the founding of the site, but rather about how to improve and expand the carding business (Glenny 2011, pp. 66-67).

Rather than there being discrepancies between these accounts, it appears likely that both meetings took place, with a possibility that there were more (UKR-(F)LE-3). While individual memories on specific details are beginning to fray, law enforcement records can confirm some major points. One law enforcement document that was furnished to me confirms the 2001 meeting in Odessa, suggesting it included over 150 mostly Eastern European criminals and that it led to the establishment of both the CarderPlanet website and the International Carders Alliance. The other meeting in 2002 was also confirmed by a US law enforcement agent checking law enforcement records, with the Odessa Hotel being the location.

Leaving aside its origins, CarderPlanet's true impact was in creating the first genuine marketplace for cybercrime. Poulsen views CarderPlanet as a "reinvention" of Counterfeit Library for the former Soviet Bloc, but with a greater emphasis on being a "disciplined online bazaar" rather than a "freewheeling discussion board" (Poulsen 2011, pp. 73-74). The other major difference was that Counterfeit Library initially focussed on fake documents, while the central part of CarderPlanet's trade involved compromised credit card details, which would become a mainstay for profit-driven cybercrime for many years.

CarderPlanet would also become a model for future forums. First, it introduced a strict hierarchy for the website, appropriating ranks from the Sicilian Mafia, including

the “Family”, “Capo di Capi” and “Capo”.[15] Many subsequent forums would employ a similar hierarchy, though often with less emotive titles. There is some variation between forums, but commonly there is one or more administrator who leads each site with the support of moderators. These officers enforce the rules coming from above and deal with day-to-day issues, perhaps with regard to managing subforums. Below the moderators are ranks of members with varying seniority and related privileges (Lusthaus 2012, p. 80). Second, and in a similar way to Counterfeit Library, CarderPlanet required that vendors pass through a review system before they could sell on the site. But where all Counterfeit Library vendors were reviewed by the administrator, the CarderPlanet hierarchy provided for approved reviewers who could perform this function, and presumably free up time for the leadership (Poulsen 2011, p. 75). Finally, CarderPlanet appears to have instigated a very important element of governance into the burgeoning economy: a cybercriminal escrow system (Glenny 2011, p. 76). This entailed the buyer and seller exchanging the payment, and sometimes goods, through a third party. It has since become a key element of the cybercrime economy, especially among Eastern European actors.

While CarderPlanet provided a model for cybercrime forums, this was not enough on its own to ensure the development of an industry. In an interview with the Russian *Hacker Magazine*, Script explained that there is no such thing as “universal carders” and that at some point each carder will need the services of another person. Part of Script’s goal was to unite these specialities to allow the business to thrive:

> Carders are actually like lone wolves, they do not gather in groups and do not organise their own networks, and they work

[15] US law enforcement document and offline archived elements of CarderPlanet.

> on their own... So-called forums are like dens of wolves; they trade information or observe offerings in some fields in order to find new solutions... (Xakep.ru 2002).

But while Eastern European carders had significant expertise and a keenly entrepreneurial spirit, they lacked one key component in their business model. Many of their targets were in the West, which meant that the money from compromised credit cards and other scams often had to be "cashed out" in the West to avoid the suspicions of Western financial institutions and banks. In many cases, purchases shipped directly to Eastern Europe would be blocked or were not even possible. Script and his colleagues needed a group of committed fraudsters in the West to carry out this aspect of the business. Counterfeit Library provided a near perfect fit. As Lance explains:

> Script and company have CarderPlanet open and it's strictly a Russian site. At the time, you've got all the information that's in Russia, but the Russians over there don't really have the ability to cash out. So stateside, it's Counterfeit Library at the time, and we're huge over in the states, but we don't have all this credit card information (NA-(F)CC-3).

The key moment was when a number of major Russian speaking players, including Script, BOA and BigBuyer, had come over to Counterfeit Library and joined as vendors:

> Up to that point we were basically just identity theft and eBay scams, small time stuff like that. Script and all these guys bring the credit card information over there and like overnight we transition more from IDs into credit card thefts (NA-(F)CC-3).

A cross germination took place. With the key CarderPlanet members vending on Counterfeit Library, CarderPlanet opened an English language section allowing some members of Counterfeit Library to ply their trade there. While not widely documented, this alliance provided some of the foundations for the development of a transnational cybercrime industry. Without the connection of the technical elements with the cashing out elements, profiting from cybercrime is very difficult. This exchange of services between cybercriminals from the East and the West remains fundamental to the structure of the cybercriminal economy up to the present. Counterfeit Library and CarderPlanet had originated the cybercrime scene online and provided the foundations for a fully-fledged industry. Where before lone wolves operated, unable to easily find partners, buyers, sellers and information, the birth of the forum scene largely solved these problems and established an online community with its own norms and understandings.

The legacy of Counterfeit Library and CarderPlanet outlived the sites themselves. Both came to an end within a few years. The former ran into to some practical difficulties and was shut down by its administrators (NA-(F)CC-3). CarderPlanet was also removed by its leaders in August 2004 after attracting too much law enforcement attention.[16] Their concerns were probably justified. Roman Vega, aka BOA, had been arrested in February 2003 in Cyprus and extradited to the United States (USDOJ 2013). Meanwhile, Dmitry Golubov, aka Script, was arrested by Ukrainian authorities in the summer of 2005. He was released only months later on the "advice" of some local Ukrainian politicians, and has now become a politician himself (Zetter 2007b). After founding the Internet Party of Ukraine in 2007 (Krebs 2008), he was later

[16] US law enforcement document.

elected to Ukrainian parliament in 2014 and, as of writing, Golubov is a member of the Petro Poroshenko Bloc (http://itd.rada.gov.ua/mps/info/page/18074).

The cybercrime industry would continue to grow after the fall of these sites. Just as the forum format developed by CarderPlanet became a model for future sites, the key players from the site moved onto other forums and began to operate there. These groupings included Mazafaka.ru, The International Association for the Advancement of Criminal Activity, Carder's Army and Carder's World among others.[17] But at the time, the most successful global imitation of CarderPlanet was ShadowCrew. This was an English language forum founded in August 2002, chiefly by Deck and Black Ops. These two figures at least partly mirrored two of the key CarderPlanet players. Following their convictions, Deck was revealed to be Andrew Mantovani, an Arizona business student in his early 20s who saw himself as the "spiritual leader" of the forum. Black Ops, like BOA, was the older partner. He was in his 40s, with prior experience as a mortgage broker (Grow and Bush 2005). The scale of their achievement was impressive with claims of reaching 4000 registered users by April 2003 and connecting a diverse set of criminals from around the world, including Eastern Europe.[18]

Some of the central players in Counterfeit Library migrated over to this new forum, just as they were shutting down their own site. They brought that experience with them and contributed to the development of ShadowCrew's review system, whereby approved vendors had to be vetted by endorsed reviewers (NA-(F)CC-3). While the site had a strong focus on carding, it also provided for a large range of other forms of

[17] Ibid.
[18] *US v. Andrew Mantovani and Others*, United States District Court, New Jersey, 2004 [indictment].

criminality. This included broader cybercrime activities like the sale of distributed denial of service attacks, as well as related activities like fake documents (in the tradition of Counterfeit Library), and those that were not related at all like the sale of drugs. The one product that was banned was child pornography (Poulsen 2011, p. 76). Such a ban is common in many cybercriminal forums. But it was probably less to do with morals and more to do with self-protection: child pornography has historically been the one cause that unites law enforcement cyber units across the world and benefits from strong political support and funding.

ShadowCrew was perhaps a victim of its own success. It soon attracted law enforcement attention and became the subject of a U.S. Secret Service investigation. Albert Gonzales (aka Cumbajohnny), a high-ranking member of the forum and a leading cybercriminal in his individual capacity, was arrested in 2003 and turned informant. Following his cooperation, Operation Firewall was carried out on October 2004 leading to the arrest of some the biggest players on ShadowCrew and the closing of the forum (USDOJ 2005). Although written to emphasise the gravity of the criminality involved, the indictment in the case illustrated the significant organisation and governance involved in a major cybercrime forum:

> Administrators collectively controlled the direction of the organization, handling day-to-day management decisions as well as long- term strategic planning for its continued viability. Administrators determined which individuals were permitted to become and remain members of Shadowcrew; the functions, responsibilities and levels of access to information for all members of the organization; and the rewards accorded members for their loyalty to Shadowcrew (e.g., elevated status within the organization) as well as the punishments meted out to members disloyal to the organization.[19]

[19] Ibid.

With Shadowcrew gone, the forum scene was disrupted. Instead of one dominant successor forum emerging, several forums competed for supremacy among the world's cybercriminals. Among these new English-speaking forums were Scandinavian Carding, the Vouched, TalkCash, DarkMarket and CardersMarket. The latter two would eventually enter into an online war of sorts documented by Poulsen in *Kingpin* (Poulsen 2011). Former members of ShadowCrew were commonly involved in these later sites. Jilsi, aka Renukanth Subramanium a Sri Lankan immigrant to Britain, was one such user of ShadowCrew and became a founding member and key administrator of DarkMarket.[20] Founded in 2005, DarkMarket operated in a similar vein to ShadowCrew. While some might call it a "Facebook for fraudsters" (BBC 2010), like other criminal forums it was more akin to eBay in its trading function, though it was also a place where cybercriminals could congregate and build some sense of community, retaining a social component along with the purely business elements. It was perhaps the largest and most successful site of its kind at the time, at least in the English speaking world, and provided a key hub for the trade of compromised credit cards, associated goods and services, along with a growing list of other cybercriminal wares (UK-LE-1, US-LE-2).

DarkMarket's central competitor in the carding business was CardersMarket, which was founded by Max Butler who had previously been associated with Shadowcrew and CarderPlanet (Poulsen 2011). Under the handle Iceman, Butler served as administrator of CardersMarket and displayed a rare skillset for someone in his

[20] *R v Renu Subramanium and John McHugh*, Blackfriars Crown Court, 2010 [Opening Note].

position: he was an elite hacker. Many other carding administrators like Jilsi are often, though not always, primarily fraudsters rather than technical operators. This seems logical given that, though some technical requirements remain, overseeing a forum is largely an operational and managerial challenge. In contrast, Butler had a fearsome reputation as a hacker and his technical abilities continue to inspire reverence and/or grudging respect from a number of the former cybercriminals I have interviewed (NA-(F)CC-2, EE-(F)CC-2).

This period is perhaps most famous for the emergence of a major cybercriminal: Master Splyntr. With a reputation as a leading Polish spammer, Splyntr eventually rose to the rank of administrator on DarkMarket. But Splyntr's rise ultimately led to the downfall of DarkMarket in 2008, along with CardersMarket, and the arrest of a number of key cybercriminal figures including Max Butler and Jilsi. Splyntr's true name was not Pavel Kaminski, as was widely believed, but Keith Mularski. Mularski was an undercover agent for the FBI based in Pittsburgh, who had successfully fabricated his online persona and fooled a number of major cybercriminals around the world (Poulsen 2011, Glenny 2011). While he wasn't the first such agent to infiltrate a major forum, in a sense, Mularski was the cyber equivalent of Joseph Pistone, who infiltrated the Bonnano crime family in 1970s New York and was on his way to being a *made man* before the FBI extracted him (Pistone 1987).

The Specialisation and Fragmentation of the Market

While English language carding forums have often attracted the most attention from writers and scholars, it is important to note the cybercrime scene is a lot more varied

than carding alone. In the early days of profit-driven cybercrime, carding was one of the most lucrative activities available and so became an immediate focus. But from CarderPlanet onwards, the carding sites themselves have not only addressed carding, even if it is their primary business. Carding forums have commonly offered other products and services including: distributed denial of service attacks, hacking tools, exploits, hacked ebay or amazon accounts, databases of personal information, hardware, hosting services, spamming services, phishing services, malware, botnet[21] rental.[22] In recent years, some attention has shifted from carding to other increasingly profitable areas like online banking fraud/theft.

Specific forums also emerged that focussed on various aspects of cybercrime. For instance, after its founding in 2008 and until its takedown in 2015, Darkode became perhaps the pre-eminent English language forum on the more technical aspects of cybercrime, such as malware and botnets. Other forums have specialised in sub areas such as hacking, zero-day vulnerabilities,[23] click fraud and spam.[24] Some focus on trade, with others limited to discussion. A number of forums are generalist and provide a broad range of subforums on various topics, while others focus largely on one core topic like spam. Part of this might be due to the value of creating specialist communities, but it is also probably an attempt to limit law enforcement interest. An administrator might ban carding from a spam or click fraud forum because these activities are sometimes viewed as legal grey areas, whereas carding is unequivocally

[21] Botnet is short for robot network. It is a network of computers that have been infected by malware and are now controlled by a bot herder. They can be used to carry out DDoS attacks, send spam, or harvest data from the victim computers.
[22] Observed from sections in a number of past forums.
[23] Vulnerabilities are essentially holes in computer software that can be exploited by attackers. A zero-day is a vulnerability that has not yet been publicly disclosed and therefore remains unpatched.
[24] Past and present examples of more specialised forums include, for instance, HackForums.net, TheRealDeal, BlackHat.World.com, Spamdot.biz.

criminal and would attract greater law enforcement attention and penalties. This is a similar approach to ShadowCrew's banning of child pornography and many carding forums refusing to allow the sale of drugs.

Forums also developed to specialise not only by subject, but also by language. Though the technical architecture may differ, over the years forums have been established that conduct business in German, Chinese, Spanish, Portuguese, Russian and more (US-LE-2, BRA-CSP-1, CHN-CSP-1). But there is little doubt that from the beginning, alongside English, the Russian language forums have been the most significant for the global market (US-CSP-14, UKR-CSP-1). Although, it is important to clarify that these forums do not cater specifically to Russian nationals, but to Russian speakers across the world and particularly those in the former Soviet Bloc. These forums are in some sense the technical engine room of global cybercrime, hosting some of the most elite hackers, coders or those representing them. As mentioned above, after the closing of CarderPlanet, many former members moved on to other forums. While some Russian speakers spent time on international boards like ShadowCrew, where they could access partners in other countries that could cash out their wares and provide other services, a number stayed with Russian orientated forums. The most successful forum in terms of reputation was Mazafaka.ru, which continues to be one of the leading Russian language forums at the time of writing. Later Russian forums that emerged and became successful include Verified and Direct Connection.

Just as in the English-language scene, more technically focussed Russian forums also emerged. These appear to stem from a different model from the CarderPlanet line,

with a strong presence of Russian nationals. Perhaps the most famous of these forums has been anti-chat.ru, which began in the early to mid 2000s and was largely a discussion forum, but developed a commercialised section over time (RUS-CSP-5, RUS-CSP-6, UKR-CSP-3). This trend also occurred in relation to other technical forums. For instance, the software cracking and reverse engineering forum reversing.net had sections on topics like viruses, but also a commercial section for trade. These commercialised sections allowed for the sale of products like exploit kits and led to an increasing specialisation within the community. An actor need not be skilled in every discipline. They could simply purchase goods/services from others with expertise in different areas (RUS-CSP-5, RUS-CSP-6).

After some time, the commercial sections developed into fully-fledged private forums, often charging an entry fee to keep out school children and low paid security researchers. These forums were increasingly specialised and often forbade activities like carding. Two Russian security researchers, Vladimir and Aleks, noted that there are many ways to make money from cybercrime and the "smarter ones" generally try and stay off the law enforcement radar (RUS-CSP-5, RUS-CSP-6). Part of this shift towards private forums may have been in response to some of the major discussion forums, like anti-chat.ru, banning commercial activities on their platforms. Igor, a Ukrainian security researcher suggested that a core of Russian-speaking cybercriminals used to come from anti-chat.ru, but that this is no longer the case. The forum is now more for learning and sharing information, rather than being closely related to business. In a similar vein, another important forum called webhack was closed entirely by its administrator, as he didn't want it morphing into a cybercriminal forum (UKR-CSP-3).

In recent years, there has been a distinct schism between the English and Russian-speaking forums. Likely tied to their post Soviet environment, Eastern European cybercriminals are often viewed as less trusting than cybercriminals from elsewhere (RUS-FSP-3, RUS-CSP-10, RUS-CSP-11). While some distrust is directed at all participants in the scene, Westerners are particularly suspicious. Part of this may stem from various forms of Soviet era propaganda, but more recent events play a key role. With the Western law enforcement pressure facing CarderPlanet and the subsequent operation against ShadowCrew, which embroiled some major Russian-speaking players, it's not surprising that much of the Russian community retreated to Russian speaking forums and they were wary of those who did not speak the language. A number of forums also have entry tests that require a knowledge of the Cyrillic alphabet or Soviet era trivia to restrict membership to supposed insiders (RUS-CSP-3, RUS-(F)LE-1, RUS-CSP-5, RUS-CSP-6). Even during the mid 2000s when DarkMarket and CardersMarket were at their peak, the Russian scene was already largely separate (Poulsen 2011, p. 128). Mularski's deep infiltration into the heart of the English language forums certainly wouldn't have helped repair the schism. In the face of law enforcement monitoring, CarderPlanet's somewhat naïve global vision seemed dead.

Nonetheless, some interaction between Eastern European cybercriminals and others remains. There is still money to be made in the global market, where the technical elite of the East can sell its wares to Western and other criminals. For instance, the leading cybercriminal and supposed author of the Blackhole exploit kit,[25] Paunch, was

[25] An exploit kit automates the exploitation of vulnerabilities in order to deliver malicious code.

active on the English language forum Darkode (Krebs 2015). While some restrictions have been lifted and new ways to monetise stolen data have emerged, cash out specialists based in Western countries are still a valuable part of the underground economy. As a result, some forums like Carder.su were built around some key Russian suppliers of credit card data or other products, with a market of buyers or partners from around the world. The interactions across geographical lines have become more cautious and guarded than in the CarderPlanet and Shadowcrew era. For instance, despite some beliefs to the contrary, the leading Russian forum Mazafaka does have some English speaking members, perhaps claiming a Russian connection. But they are not expected to gain much trust from the community or go particularly far in terms of business (ROM-(F)LE-1, NA-(F)CC-2, UKR-(F)LE-2). Scott, a former North American cash out expert, who engaged in the activity full-time and at a high level, wrote about it this way:

> Mazafaka was supposed to be only for Russian speaking people etc. I had been on it alot but if you didnt speak russian it was not really best place for english speakers. Alot of the serious russians wanted to start dealing with only people that spoke fluent russian because it was kind of a way for them to feel more comfortable that you were not a U.S. law enforcement guy etc. (altho that in no-way assures it). They could tell fakes trying to use Google translate etc because they could never speak fluent russian slang (NA-(F)CC-2).

The profound effect of law enforcement pressure on cybercriminal forums has not been limited to Russian speaking cybercriminals. With the operation against ShadowCrew involving a key Secret Service informant and DarkMarket eventually being run by an undercover FBI agent, cybercriminals have become very suspicious of major forums in general. Scott had been a member of forums since the

CarderPlanet days, but over time attempted to limit his involvement with them where possible:

> Around the time the forums IAACA and DarkMarket (sting site) were around, I kinda fell off of the forums because I no longer needed them and felt like there was too much heat on them after the Shadowcrew bust in 2004. I had already made a bunch of contacts and didnt really have a need for the forums any longer, so I just chatted with the partners I already had on ICQ and IRC etc. I eventually got back involved with forums (i.e. XXXX)[26] later on when most of the people I had known for years eventually disappeared (busted, retired etc) and I needed some new contacts. There were still several people I had known for years that I talked to alot, but most were scared to be on any forums anymore like I said so alot of people were no longer participating in them. There were also other forums that they WERE on, and myself included, but its probably best that I don't elaborate on that. They were more "elite" in general and more "closed" so I guess people felt they were more safe (NA-(F)CC-2).

Scott also hones in on the central purpose of forums within the cybercriminal community. Rather than being the essence of the scene, they are primarily a place to network for those who do not have sufficient contacts. In the current environment, undercover law enforcement agents and security researchers are well entrenched in the major forums. These meeting places now appear to be something of a necessary evil that one only uses when there is no other choice. This is a common view amongst former cybercriminals that I have interviewed. Lance viewed forums with some suspicion, even after being closely involved in establishing a number of them. While ShadowCrew was operating, Lance was making considerable income from other forms of fraud that didn't require online partners. At this point, word began to spread about law enforcement interest in ShadowCrew and particularly some of the members

[26] Redacted to maintain anonymity.

connected to him, so Lance took the opportunity to retire from the forum and gradually phased out much of his online presence elsewhere (NA-(F)CC-3).

Nonetheless, large forums continue to operate in both the English and Russian language scenes. Examples have included the Russian stalwarts like Mazafaka and Direct Connection, along with a number of English focussed sites like Ghostmarket, Kurupt.su, Carder.su and Omerta among others. These latter sites have generally faced greater pressure from law enforcement, often leading to arrests and website takedowns, with new sites emerging over time. But the preference among the connected now seems to be for smaller more secure groupings. Scott elaborated a little further on what these groupings look like:

> As for the more "elite" closed forums etc there was really nothing different about them at the time other than it was just more secretive among the known people that were trusted for awhile. Some were only known to people in their "inner circle". Some only were for Russians etc…
> …As for the number of members on some of the other forums.....I dont remember for sure but we are talking number in the 100's as opposed to 1000's.....I remember one hacking forum with as low as 80 something members I think (and some of those are multiple logins from same people im sure) (NA-(F)CC-2).

The organisation of profit-driven cybercrime has almost gone full circle. Some cybercriminals have even reverted to small chat groups that were in vogue before the rise of Counterfeit Library and CarderPlanet. At the time of writing, Jabber was a particularly common platform currently being used by a number of cybercriminals (US-LE-2).

The Development of Operational Structures

Of course, the history of profit-driven cybercrime is not only the history of marketplaces. Forums play an important role in the industry, but they are far from the only organisational structure that has evolved. One should also consider groupings that actively carry out aspects of cybercrime, rather than simply engage in trade. With that said, forums likely enhanced the development of these other facets of the business. For instance, Script envisaged forums as a den for lone wolves to meet, but once they met it's not surprising that wolf packs formed. In practical terms, one of the most common cybercriminal group structures is akin to a crew. Just like a bank robbery crew, a cybercrime crew involves a small number of individuals with particular roles.

Maksym, who monitors the Russian-speaking underground, gave an example of the structure of a malware production group, but he stressed that there is no one-size-fits all model. In this example, there is a *boss* who is likely the original author of a piece of code and its owner. The boss may hire a software developer to work on aspects of the code, in the same way legitimate coders sometimes require help from others due to time restrictions, the amount of work involved, or the specialist nature of the programming required. This developer is kept on salary by the boss. The boss and the developer bring the malware to fruition, but the boss also hires two or so sellers to bring that product to market. These sellers are on salary, but may also be paid a commission based on sales. Maksym believed such groups could work together successfully over a time span of months, but that a year was usually the longest they could hold together before various "disruptions" occurred (UKR-CSP-1).

Certain crews may also operate together in an offline capacity, either meeting on forums in the first instance, or else in their local community or through mutual acquaintances. For instance, Albert Gonzales, one of the most infamous and highest earning American cybercriminals of all time, had a number of associates that he operated with in person, both for business and socialising. One of their main activities was "war-driving", which involved driving past or positioning themselves near the WIFI signals of major "big box" stores in order to access the network and steal credit card information (Verini 2010). But the most obvious case of offline organisation that has developed with the rise of cybercrime is the cash out crew. Such groups are charged with converting virtual gains into money or physical products. By virtue of the physical nature of the work, often involving making physical purchases from shops or withdrawing money from ATMs, it is not surprising that a number of such offenders are known to each other (NA-(F)CC-2). While there are some examples to the contrary, the organiser of each crew often recruits those known to him or others he trusts in the community, some of whom might come from a broader background of criminality (WE-(F)CC-1, NA-(F)CC-2, UKR-CSP-3).

Some examples go beyond crews and suggest structures that have developed to approximate illicit companies. For instance, in 2012, a group of cybercriminals was arrested in Moscow making use of Carberp malware to steal tens of millions of rubles from online bank accounts. Led by two brothers, the group rented office space and appeared externally to be a legitimate technology company (Ragan 2012). In the context of spam, Brian Krebs profiled some of the leading spam operations of recent years in Russia, providing great detail on how business-like they are, with official

places of business, hierarchies, and employed staff (Krebs 2014). It should be noted that spam falls into particular legal categories depending on the jurisdiction, but in Eastern Europe they are generally regarded as being in a fringe area of legality allowing somewhat grey enterprises to operate. Overall, it is clear that operational structures have evolved alongside the development of the broader industry. In fact, all these groupings really fall under the concept of *firms*. This will be discussed more directly in the next chapter.

The Growth of Cybercriminal "Infrastructure"

Another important facet of the evolution of profit-driven cybercrime has been the growth of what might be called the economic infrastructure of cybercrime. For instance, this has included functions like the development of virtual currencies, along with the hosting of illegal content and operations. Virtual currencies have been a vital aspect of the expansion of profit-driven cybercrime. Without a functioning monetary system, widespread trade and payment online would have been very difficult to facilitate. In the early days, the Russian company WebMoney offered a solution to this problem. Founded in 1998, it began operating just at the time when the nascent cybercrime industry was itself emerging and was widely used for online payments on CarderPlanet (USDOJ 2013). The security researchers Vladimir and Aleks described the importance of WebMoney with regard to cybercrime by comparing its significance to that of *hawala*, the money transfer system that facilitated the flowering of trade out of the Islamic world in the medieval period (RUS-CSP-5, RUS-CSP-6).

Other virtual currencies have also been adopted by cybercriminals. These have included E-gold, Liberty Reserve and Perfect Money. The attraction of these

currencies is that they often operate out of non-Western jurisdictions. They are ostensibly beyond the reach of Western regulators or law enforcement, who might try and "interfere" with the service. Equally important is that they are loosely regulated and require little if any information on the true identities of their users, allowing pseudonymous transfers. Founded in 2006, the Costa Rica based Liberty Reserve was a good example of such practices and became perhaps the leading cybercriminal currency until it was shut down by the U.S. Secret Service led multi-country investigation in 2013.[27] Following the death of Liberty Reserve, bitcoin has become an increasingly important currency among cybercriminals, because it offers similar benefits to the other virtual currencies in terms of maintaining anonymity, but has the added advantage of being decentralised (US-LE-8).

The evolution of cybercrime also owes much to another facet of technical infrastructure: bulletproof hosting. A bulletproof host is quite similar to a standard Internet service provider (ISP), but specialises in hosting activities and businesses that would be deemed illegal in a number of jurisdictions. They refuse requests to shut down the hosting of the offenders. The most famous of these enterprises was the Russian Business Network (RBN), which was perceived as a cyber boogie man for a number of years, and a regular suspect in much cybercriminal activity, even if their actual involvement was sometimes unlikely. The history of RBN is very shadowy, partly because a number of researchers and writers chose not to comment publicly on the group for fear of reprisals (US-CSP-14). Part of this appears to be linked to concerns that RBN is connected to the Russian mafia, but these claims remain equally unclear given the lack of published material on the subject. The commonly agreed

[27] *US v. Liberty Reserve S.A. and Others*, United States District Court, Southern District of New York, 2013 [indictment].

facts have been that RBN's primary business was as a bulletproof hosting provider and they appeared to operate out of a hub in St Petersburg (Graham 2009, pp. 171-172). They played a very extensive role in the market and were regularly implicated in supporting a large number of cybercriminal enterprises (Krebs 2007).

Drawing on Russian-language sources, Krebs (2014) provides some rare details on the history of RBN. He traces the group's origins to Minsk in the early 2000s and, in particular, to a young Belarusian named Alexander Rubatsky, whose father was a high-ranking police officer. Rubatsky was a talented technologist and quickly became associated with local organised crime groups, whom he assisted with various money-making schemes that required his skills. But he had his real start specialising in payment processing for sites selling child pornography. In 2004 he fled to St Petersburg after his organised crime associates kidnapped a rival businessman, who was moving into the same business, and were arrested. After a failed attempt at a new payment processing enterprise, Rubatsky shifted into hosting instead, partnering up with a Russian ISP called Eltel. According to Krebs' account, the company had previously hosted child pornography and was under the protection of certain Russian law enforcement agents. Rubatsky's contribution was to establish a direct link to major Tier 1 Internet backbone providers, making Eltel less susceptible to being shut down by intermediary ISPs. They called this Internet pipeline the Russian Business Network and placed a young hacker known as Flyman in charge of it (see Krebs 2014, pp. 17-24). Flyman would become an infamous name in relation to RBN and is suspected of having his own strong political connections through his father, "who occupies a position of influence at a key Russian ministry" (Graham 2009, p. 173).

RBN would eventually disintegrate after gaining too much public attention and facing difficulties from upstream providers. It officially dissolved in late 2007 (Graham 2009, pp. 202-207). Of course, bulletproof hosting did not cease to exist at this point, it merely became less brazen and often carried out by smaller, less centralised, enterprises. Such companies have included Atrivo, McColo, 3FN and a number of others. Some also believe that certain members of RBN continue to operate in the same market or are involved in other forms of cybercrime to this day (US-CSP-14).

The Current State of Cybercrime and Cybercriminals

Cybercrime is an amorphous and constantly changing phenomenon. As new technologies emerge, new attack vectors and scams become available. Thus far, some of the major forms of cybercrime have involved credit card fraud, the theft of data and money, extortion against companies through targeting their online business portals, confidence scams of varying types, and illegal marketing in the form of spam. As noted in the introduction, cybercrime is not something vastly new, but is rather the leveraging of new technologies to carry out existing forms of crime. The difference is in the expression of those crimes, through new methods and perhaps carried out by novel actors, rather than in the crime types themselves. With so many opportunities available, and technology evolving quickly, it is almost impossible to develop a taxonomy of the subtypes of cybercrime that have emerged. It is a near limitless terrain. If there is money to be made, someone will devise a way to make it. Dave, a hacker who was previously involved in a boutique “niche fetish porn” spam enterprise, illustrates this point perfectly:

> Do you know what my biggest spinner was? It's called balloon pop pornography. It's basically a girl, she's fully clothed - Japanese, it has to be Japanese - she's wearing an office uniform, white blouse, pencil pleat skirt, pantyhose, she's sitting on a balloon. And you see a hand with a pin. It gets closer and draws away. Then it gets closer…pop! That was it. So what I did was I hacked all the sites that did this, like all of them and I got all their customer bases.[28] I started spamming just one of them from all of them. I got 33 per cent of people to sign up to it. 33 per cent return on spam is fucking insane… because it's so niche, so fetish, Japanese businessmen… (SEA(E)-(F)CC-1).

Of course the whole business was a scam and the pornographic product being advertised was never provided.

Instead of providing a taxonomy of cybercrime, a broader view of the overall system might be useful. In this regard, there is almost universal agreement among subjects I have interviewed that over time cybercrime has been growing more organised and sophisticated (US-(F)LE-2, UKR-CSP-1). It is now extremely business-like in its operation and has developed into a bona fide industry. Carter, a U.S. law enforcement agent with considerable experience in the cyber underground, summarised developments in this way:

> It's more sophisticated, for one. With every law enforcement action, the criminals they adjust. So it's very sophisticated. I think some of the money they are dealing with is staggering. I think more of it now is malware based cybercrime. Whereas before it wasn't as much. It is very malware based and very highly sophisticated, you know with the different types of obfuscation techniques you could utilise. I guess probably one of the best ways I could describe it is more automated. There is for example, in 2005, if you were going to be doing infections, you would have a zero day vulnerability you would have one and take advantage of that. Now you can go out and buy an exploit kit that has twelve vulnerabilities in there and you would

[28] Databases.

> just drive traffic to the site and it infects people. Whereas before you would maybe have to have an executable and have them click on it to get infections. And you would have to know how to script all that stuff. Now I just buy the kit and drive traffic to it. Now I just buy the malware – I don't even need to buy the malware, I can buy the malware as a service right now and say hey I am going to pay 300 dollars a month to have access to it, kind of like lease it. Everything I think is more automated. Even right down to vendings, they have these automated vending carts so like for selling compromised credentials, like credit cards or bank logins, or things like that. Whereas in the past, I would have to reach out to you and do business with you personally on instant messaging and I would pay you. But now they kind of have like store fronts kind of like buying a pair of shoes online. You visit the website you, set up an account with an email address, and you go and it's a drop down menu, go through the checkout process and it's automated payment where I would never even talk to you or know who is even behind it. Very automated (US-LE-2).

The profiles of contemporary cybercriminals also suggest this shift towards sophistication, specialisation and ultimately corporatisation. In the early days of cybercrime, before wide scale profit-driven activities truly existed, the scene was made up of hackers and *phreakers* who had some technical skills. A number were quite young, particularly those that had run-ins with the law. But with an industry centred on profit, hackers and coders are now only one facet of the system, along with a new breed of fraudsters and conventional criminals of various stripes. Tom, a UK law enforcement agent, questioned the old "stereotype of a 15-year-old sitting in a darkened room". In his experience, cybercrime offenders reflected a cross section of society (UK-LE-1). As noted previously, Carter has come to a similar conclusion based on his experience in the field: "About the only profile that I can probably say is that they're male" (US-LE-2).

Conclusion

This chapter has charted the evolution of profit-driven cybercrime. It outlined the early history of hacking from the late 1950s onwards, from which some key aspects of cybercrime emerged, and then focussed on the turn towards profit-making activities in the 1990s. The chapter provided an overview of the evolution of forums from their birth and Golden Age in the 2000s through to their increasing specialisation and fragmentation. It then drew attention to the development of other aspects of the industry such as operational groupings and the cybercriminal "infrastructure" that underpins the economy, like virtual currencies and bulletproof hosting. The final section addressed the current state of cybercrime and cybercriminals.

The central feature of contemporary cybercrime is that it is industrialised. This is the subject of the next chapter, which takes a more analytical focus framing cybercrime in terms of industrial organisation. But it is already clear from this chapter that like many aspects of legitimate business, cybercrime relies on a competitive market where individuals and firms seek profits by specialising in valuable aspects of the business. At the heart of this, and from the beginning of financially motivated cybercrime, there has been a fusion between technical and criminal minds. As noted above, where money is to be made a new expression of cybercrime will likely emerge. Old firms will evolve and new firms will spring up to meet different demands. Given that a considerable part of this industry takes place online and outside licit channels, there will likely always be a certain amount of flux within the market. How cybercriminals manage these challenges and their inherent instability is the subject of chapters 5-8. While the market will never function perfectly, it certainly provides a suitable den so

the wolves don’t need to be alone anymore.

4. Making Sense of the Cybercrime Industry

The previous chapter outlined the industrialisation of cybercrime in a historical sense. Drawing on key issues that emerged out of that account, the present chapter continues to argue that cybercrime has become an industry, but does so this time from an analytical perspective. From the previous chapter it should already be clear that cybercrime constitutes an industry because there are a number of (illicit) businesses operating for much the same effect and in similar ways. This chapter takes matters one step further by attempting to make sense of central aspects of cybercrime and how they work together within a framework of commercial behaviour. It achieves this by broadly applying some fundamental ideas within economics and industrial organisation in particular, which is chiefly concerned with the operation of firms and markets (Church and Ware 2000, Hay and Morris 1979). As part of this application, this chapter also seeks to illuminate some core aspects of cybercrime that have not been well understood up to this point. The central issues explored in this chapter include: 1) the specialisation of cybercrime; 3) the professionalisation of cybercrime; 2) an examination of cybercriminal markets; 3) an outline of cybercriminal firms.

Specialisation

There is among cybercriminals a clearly evident division of labour. This concept, central to foundational economic thought, holds that specific tasks in an economy can be separated from each other and thereby specialisation occurs. This then dovetails into the formation of firms and/or trading within the market to benefit from the skills

and goods that other specialised workers can provide. It also generally leads to an increase in levels of production. Taking the famous example of pin-making, Adam Smith outlines how this process works:

> a workman not educated to this business (which the division of labour has rendered a distinct trade), nor acquainted with the use of the machinery employed in it (to the invention of which the same division of labour has probably given occasion), could scarce, perhaps, with his utmost industry, make one pin in a day, and certainly could not make twenty. But in the way in which this business is now carried on, not only the whole work is a peculiar trade, but it is divided into a number of branches, of which the greater part are likewise peculiar trades. One man draws out the wire; another straights it; a third cuts it; a fourth points it; a fifth grinds it at the top for receiving the head; to make the head requires two or three distinct operations; to put it on is a peculiar business; to whiten the pins is another; it is even a trade by itself to put them into the paper; and the important business of making a pin is, in this manner, divided into about eighteen distinct operations, which, in some manufactories, are all performed by distinct hands, though in others the same man will sometimes perform two or three of them. I have seen a small manufactory of this kind, where ten men only were employed, and where some of them consequently performed two or three distinct operations. But though they were very poor, and therefore but indifferently accommodated with the necessary machinery, they could, when they exerted themselves, make among them about twelve pounds of pins in a day. There are in a pound upwards of four thousand pins of a middling size. Those ten persons, therefore, could make among them upwards of forty-eight thousand pins in a day. Each person, therefore, making a tenth part of forty-eight thousand pins, might be considered as making four thousand eight hundred pins in a day. But if they had all wrought separately and independently, and without any of them having been educated to this peculiar business, they certainly could not each of them have made twenty, perhaps not one pin in a day; that is, certainly, not the two hundred and fortieth, perhaps not the four thousand eight hundredth, part of what they are at present capable of performing, in consequence of a proper division and combination of their different operations (Smith 1999 [1776], pp. 109-110).

The last chapter provided a history of cybercrime that mirrors this process.

Cybercriminals moved from operating largely as lone wolves, to trading and forming groupings, which expanded their productivity on a wide scale. A core part of this process was specialisation, but it can be difficult to determine whether the development of marketplaces drove specialisation, the other way around, or both. However this process occurred, there is now a demand for a number of goods and services that require very particular skills. An actor might want to purchase malware from skilled coders, and hire others who are experienced at infecting computers. Among other means, this might require social engineering skills or the help of professional translators to produce compelling emails to send to victims. The actor might also need a transfer team to move money out of compromised bank accounts and perhaps even hire a professional con artist to convince the relevant bank that the transfers are legitimate (Lawrence 2015). Of course, then a cash out crew is required to extract the money and return the proceeds to the organiser. At this point money launderers may also play a role. Within all these specialisations, are also sub-specialties. For instance, coders might specialise in particular programming languages or different components of the malware they are writing. Such sub-specialities might be incorporated within certain firms to achieve better products, which is the subject of a later section.

Following on from Durkheim (2013 [1893]), the nature of specialisation may actually lead to a form of social solidarity among cybercriminals. Contrasted with "mechanical" solidarity, which is prevalent among small-scale societies and dependent on the homogeneity of their existence (work, kinship and so on), "organic" solidarity derives from the interdependence that results from specialisation. Durkheim believed that in modern industrial societies, members have to rely on others to provide

them with the goods and services needed to succeed in their own work. Each has their own special role to play within the broader societal "organism". In relation to cybercrime, this would support the idea that there's a level of solidarity within the industry, beyond atomised actors simply seeking economic gain. With regard to such organic solidarity. the implications for law and order are that industrialised societies are likely to exhibit an approach to justice based on restitution rather than strict punishment. It is interesting to observe the connections between this idea and the mechanisms for cybercriminal cooperation discussed in chapter 6. While the online nature of dealings and the protection that anonymity affords make stiff punishments difficult, there is a clear reliance on systems of arbitration and other tools that aim at restoring trust in the community and the normal functioning of trade.

Specialisation can also occur geographically. In meta-histories of economic development, such specialisation occurs following the development of long distance trade (North 1991, p. 99). A similar process appears to apply to cybercrime. The expansion of trade through access to online marketplaces allows cybercriminals to benefit from the skills of others. Such trade favours those who invest in developing a particular form of expertise which can become valuable as part of exchange. The fact that the cybercriminal industry is global and that actors from different countries can collaborate and trade online, means that this specialisation also takes on a regional character. It appears that the expertise specific nationalities might develop is often tied to existing socio-economic and cultural conditions. After all, every cybercriminal physically exists in a certain location. As much as they adapt to the market, the market also adapts to them. Ignoring this geographical dimension of cybercrime, means that one fails to comprehend the economic and cultural factors playing into the

structure of cybercrime operations in different countries, the nature of local participants and the specific ways they contribute to the overall industry.

For instance, it is not random that Eastern Europe provides much of the technical engine of global cybercrime. From the early CarderPlanet days, it was those from the region who drove innovation in the carding business. In recent years, some of the leading pieces of malware have been created and written by Eastern Europeans. It is these skills that Eastern Europeans are known for in the industry and that they can offer in exchange (NA-(F)CC-2). But this specialisation appears to be tied to the socio-economic context across much of the former Soviet Union and other former communist states in the region. In these places there was a strong interest and investment in science and technology: it was a matter of official policy originating with Lenin himself. Part of the effect of this approach was that education in STEM disciplines was at a very high standard, with a number of top universities in these areas producing a large supply of good quality graduates (on the Soviets and science see Bailes 1978, Graham 1993, 1998).

The second interesting element of recent Eastern European history was that, through trade embargoes during the communist period, Western technology was often out of reach. As a result, substantial efforts took place to replicate those technologies that had not already been developed locally. For instance, in Romania, Ceausescu oversaw the reverse engineering of early foreign computers, so that a local version could be produced. During fieldwork in the country, it seemed these technical achievements were a national badge of honour for some locals. With regard to software, cracking and piracy became prevalent across the region, as it has in large parts of the world.

One might view such behaviour negatively, but in a number of cases it appears these activities originally took place because the relevant software could not be easily obtained. This was usually because the software was not marketed in that country or the low local wages made it practically unaffordable (UK-CSP-4, RUS-CSP-5, RUS-CSP-6). Eventually a tradition developed and a community of crackers emerged, with a true skill for software reverse engineering (RUS-CSP-5, RUS-CSP-6). This is precisely the skill set required for success in a number of technical aspects of cybercrime.

While a large talent pool of technically educated graduates, alongside a tradition of cracking and reverse engineering, provides a supply of those who could engage in cybercrime, it is somewhat presumptuous, and offensive, to assume that they will. Individual personalities/backgrounds likely play an important role, but the lack of well paying jobs in Eastern European technology sectors and in general across other sectors provides a "push" for people to involve themselves in cybercrime. This was a point I heard many times from interview subjects across Eastern Europe, and, less relevantly, elsewhere around the globe (RUS-CSP-5, RUS-CSP-6, UKR-(F)LE-2). Some would knowingly take part in cybercrime as a full-time or part-time source of income. Others might simply be un(der)employed programmers who respond to online advertisements to assist on projects that they either don't realise are illegal, find it pertinent not to address the issue, or are simply happy to be involved (RUS-CSP-13).

As a contrasting view, it is important to note that some working in the local tech sectors believed that there were enough high paying jobs and that the situation in

Eastern Europe compared relatively favourably to other parts of Europe, especially when factoring the local cost of living (UKR-CSP-2). These views were in the minority and perhaps reflect the perspective of those who have managed to gain good legitimate employment, work hard and find criminal activity morally unacceptable. Furthermore, while salaries on offer might constitute a living or even good wage in countries like Ukraine, they often cannot match incomes that could be derived in the American technology industry or in cybercrime. In essence, cybercrime is an aspirational endeavour. In many cases, offenders have a degree of education and access to technology that moves them beyond drivers of simple desperation. For some, making a decent living may not be enough when one seeks to make a fortune like those in Silicon Valley. Vasily, a former Russian law enforcement agent, viewed things in such a way. He believed that there wasn't a space for tech entrepreneurs and start ups in the Russian economy, still encumbered by its communist heritage and dominated by a small number of large corporations, and by government and oligarchical interests. Those with a more dynamic instinct are effectively forced to create cybercriminal businesses instead. They are a new breed of entrepreneurs.

The final piece of the Eastern European puzzle is a factor common to many parts of the globe: corruption. Corruption is rife across the region and was a regular topic of discussion in interviews, including with those from law enforcement backgrounds (ROM-(F)LE-1, UKR-(F)LE-2). Subjects made it clear to me that the identities of a number of major cybercriminals are likely known by various law enforcement and private sector investigators (UKR-(F)LE-2). Yet these individuals are only sporadically arrested. It cannot be forgotten that Eastern European cybercriminals function in an often corrupt environment. It partly explains how they can operate with

virtual impunity if they navigate the system correctly. But in some ways, it also explains their career choices when the government might be perceived as just as compromised as the cybercrime scene, and simply trying to engage in legal business often brings a number of moral compromises (e.g. in the form of required bribes and kickbacks). In fact, Kirill, a Ukrainian government agent, suggested that some of those involved in cybercrime might view their criminal collaborators as quite trustworthy and rule abiding in the face of a fundamentally broken state (UKR-LE-2).

This discussion of Eastern Europe is illustrative of the importance of geographical context in understanding regional specialisation. Yet it is important to remember that cybercrime is a global phenomenon, not just an Eastern European one, as can be forcefully pointed out by some in that region (RUS-CSP-2). The flavour of cybercrime will differ in each case. For instance, Romania provides a compelling counterpoint to other parts of Eastern Europe. It benefits from its former communist heritage of heavy investment in technology, in both infrastructure and human terms. It continues to be ranked at the top of global Internet connectivity and speed rankings (Belson 2015). And it is undoubted that Romania also tops global lists as a major producer of cybercrime. But the local form of cybercrime is quite different from other parts of Eastern Europe. It is often far less technical and is centred largely on social engineering scams, such as selling fake goods on online auction sites like eBay. Romania still has the technical talent pool, history of cracking/reverse engineering and endemic though lessening corruption. But it also has a thriving tech sector and access to the rest of the EU job market, that appears to be reducing this form of more technical cybercrime (ROM-(F)LE-1). The Romanian case is more about fraudsters gaining access to the Internet than it is about an oversupply of technical talent and a

lack of suitable employment opportunities. Background discussions indicated that there may still be an unemployment problem in parts of Romania that contributes to cybercrime, but it is not a specific concern of the technology sector in the same way that it is in other parts of Eastern Europe.

Similar variations can be expected around the world. The Nigerian case may have something in common with Romania, at least on the fraud side. The poor economy, relatively good/accessible Internet and a corrupt environment provide a breeding ground for online crime. In this case, there is not a technology sector at the same level as Romania, but there is also not a large supply of technical talent on an equivalent scale. Without the large pool of programmers and hackers seen in other countries, it is not surprising that many opt for low-tech scams or have to rely on foreign actors for technical assistance (NIG-(F)LE-1). There appears to be a direct connection between the email scams that emerged in the 1990s and previously existing letter campaigns to the same effect (NIG-ITP-1). This suggests that cybercrime in Nigeria largely grew out of a community of fraudsters rather than hackers or other more technical actors.

Meanwhile China provides a different example of cybercrime again. China gains attention for hacking and government endorsed cyber-espionage, but little attention is given to specific cases of cybercrime. Surprisingly, given oft-expressed vague fears of Chinese cybercrime, local conditions mean that profit-driven cybercrime is not a major concern. Internally, the theft of online gaming credits is one of the key problems and there is only limited engagement with the global cybercrime scene (CHN(E)-CSP-1). A more focussed study on why this is the case could be fruitful: hypotheses might point to the lack of local cybercrime being due to strong patriotism

among Chinese hackers (on Chinese hackers see Henderson 2007). This is a counterpoint to the common perception of hackers, at least in the West, as being strongly anti-authoritarian and counter-culture. Other explanations for the low threat of Chinese cybercrime might relate to the close government monitoring of the Internet, as well as Chinese e-commerce still being in its infancy and credit cards and online banking not being widely used. Language barriers and difficulties in cashing out from vastly different financial systems might also limit cybercrime activities against foreign targets (CHN-CSP-1, CHN(E)-CSP-1). But this may change over time.

Finally, one cannot leave the West out of this discussion. While the West has produced a significant number of elite hackers, such as Max Butler, many are deterred by law enforcement and enter the technology sector where opportunities now abound (SEA(E)-(F)CC-1). Anecdotally, the profile of Western cybercriminals is quite different from those of Eastern Europe, with enrolment in higher education appearing less frequently (WE-(F)CC-1, SEA(E)-(F)CC-1, NA-(F)CC-2). The burning core of Western cybercrime is made up of those who can handle the money side of the business. As was noted in the previous chapter, these individuals have been some of the key players involved in cashing out in the United States and elsewhere. They are also some of the key buyers working with the major suppliers of Eastern Europe. Even some Western cybercriminals like Scott, who have technical abilities, realise that they can make more money specialising in cashing out (NA-(F)CC-2). While the East provides the technical engine of cybercrime, the West provides much of the fuel through facilitating a central part of the money side of cybercrime. In a sense, they are a near perfect match for exchange. Without Western cybercriminals, the industry

would likely be far smaller and less successful. This symbiotic relationship is a perfect illustration of geographical specialisation that one would expect in broader economic development (North 1991).

Professionalisation

The process of specialisation is mirrored by a process of professionalisation (on professionalisation, see Parker 1981, ch 12, Timperley and Osbaldeston 1975, Johnson 2016, ch 2). While some dabbling still occurs, in a number of contexts, many cybercriminals approach the business as either a full time job or certainly a significant secondary job that supplements their income (RUS-CSP-13, NA-(F)CC-2, EE-(F)CC-2, UKR-CSP-1). There was a clear division in my sample between those who engaged in cybercrime as a secondary activity and those who relied on it as their main form of employment. This appeared to be tied very closely to age, with the mid 20s as the peak of the age range for many involved in criminality. Those former cybercriminals I interviewed who had never been arrested had generally gravitated away from cybercrime in their twenties as other life opportunities took hold, whether this be undergraduate education or full-time employment. It simply stopped being practical for a number to engage in cybercrime any longer, as they began to settle down in their lives. In at least one case, one of the driving factors for quitting cybercrime was potential shame:

> When I was doing illegal things I always freaked out, mostly because I was a kid, but I always thought I was going to get busted. My parents are going to be so disappointed, I'm going to go to gaol. Everything they said is going to come true. So it's good to be legit (SEA(E)-(F)CC-1).

For those that had been arrested, factors outside their control removed them from cybercrime. As a result, it is difficult to determine when, if ever, they might have retired from the business on their own. But there appeared to be a clear choice made. Either one largely left the business and attempted to find a suitable job in the legitimate sector, or one became a professional cybercriminal and pursued that business as their primary job.

Within geographical contexts where arrest is a far lesser threat and engagement in cybercrime might be viewed in a less shameful way, there is a lower incentive to leave cybercrime at a young age. The employment situation also functions differently in various regions. For instance, in Eastern Europe, while some jobs might offer an alternative to cybercrime, a number of cybercriminals use employment as a cover for their illicit activities. Sometimes this is informal in the case of freelance programmers or those who run their own business, but in other cases they hold legitimate jobs at the same time (RUS-CSP-8, UKR-CSP-1). In fact, it was suggested to me that some of the leading criminal coders behind high level malware have been involved in the scene from the early days but continue their involvement despite being middle aged with families and holding down legitimate jobs (UKR-CSP-1).

Cybercrime is also not attracting the dregs of society, but includes intelligent, educated and able offenders. Some might downplay the technical ability of cybercriminals in relation to programmers working in the legitimate sector. There are arguments on both sides of that issue, but the real point of comparison here should be between the intellectual ability of cybercriminals and other more conventional

criminals. There is no better illustration of this point than in the Eastern European context, where cybercriminals regularly have a university education. On the technical side, there are unemployed or underemployed coders who become part of the illicit industry for either short or long periods. They share a number of similarities with coders who have gained legitimate employment because some of them are the same people (RUS-CSP-13). There is also a class of cybercriminal entrepreneurs and managers creating their own illicit startups when legitimate money-making avenues on that scale are less available. One such individual I spoke to, Fyodor, had a good general education and was very well read, regularly making references to famous political thinkers and literary figures in our discussions (EE-(F)CC-2). Romanian law enforcement also noted that a number of the fraudsters in the hub of Ramnicu Valcea, who are generally involved in less technical enterprises, are "smart guys" who often have university educations but poor job prospects in the area.

In the West, the situation is slightly different. Due to greater enforcement and increased employment opportunities in the technology sector and more broadly, many university-educated (and non university-educated) hackers have a better likelihood of finding legitimate and appealing jobs. As such, it appears rarer for Western cybercriminals to be university educated, although there are some cases of this. Among the cybercriminals from Western backgrounds I spoke to, only two had attended university. The second quit his involvement in illegality during his studies. One Russian security researcher dismissed this lack of education as a serious flaw in the quality of Western cybercriminals (RUS-CSP-8). The situation is perhaps backwards, in that the real concern is the large number of Eastern European cybercriminals who have not been successfully diverted into other occupations, not

that Western cybercriminals should be better educated and more skilled!

But while a number of Western cybercriminals lack a university education, they do not lack intelligence. A number of individuals interviewed had impressive hacking and coding skills and some had later found employment in good jobs in the technology sector. Among those with some hacking background that I spoke with, a number demonstrated a keen intelligence of a very specific kind. This links back to the hacker mindset discussed earlier. Many described the importance of the intellectual challenge of hacking, rather than only the financial payoff:

> There is challenge, respect, the thrill of it, out of doing it. The respect you get from it. How well you can do it, how quickly. There are so many different aspects. I don't ever recall saying to myself oh my god I just made 2 grand in one day. It was usually a case of oh my god I've just managed to get 20000 cards or 2 grands worth of equipment in one day. It was never I've got this amount of money in my hand. The money was almost a byproduct from it, I was always more proud about what I had managed to physically manifest from it rather than the money that came out of it (WE-(F)CC-1).

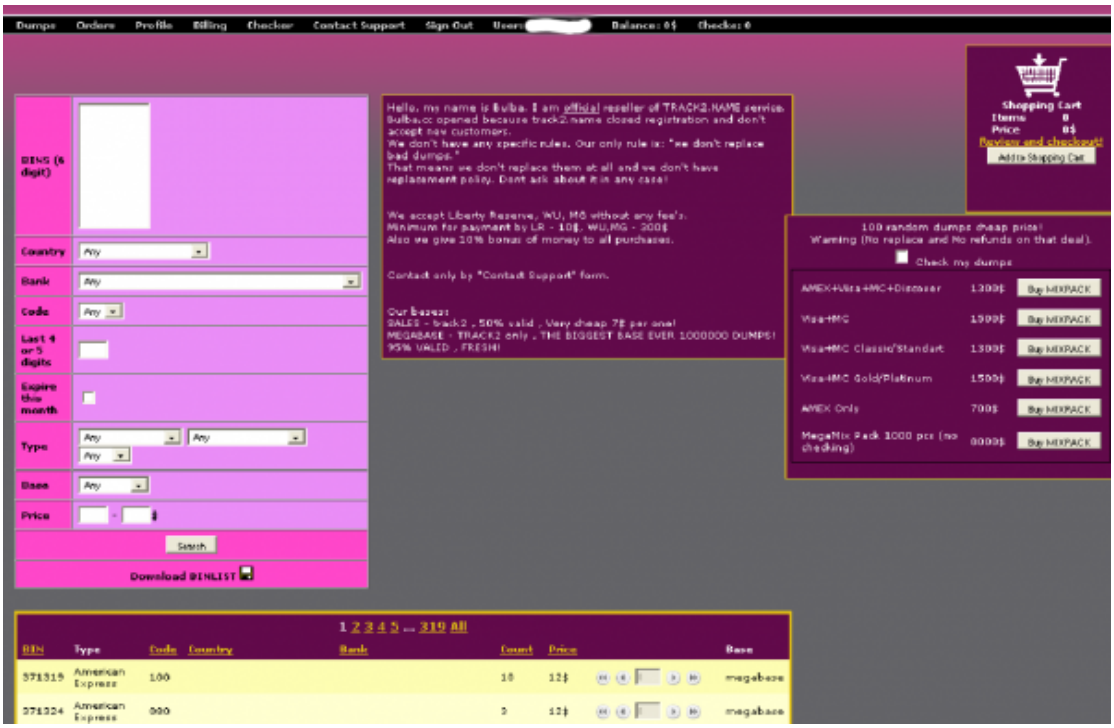
While he specialised in cashing out, Scott also demonstrated hacking traits and had an interest in the problem-solving component of cybercrime. This is his vivid account about why his activities were more than only about money for him. He wrote:

> When I was hacking or phishing I used to love tweaking my methods and getting better and better at it to increase the results. The increased results to me were not really about dollar signs in my head but how good I could do at it and how many accounts or whatever I could obtain. I guess how well I could "beat the system" (Look what I can do!! sorta thing ha). I used to do allot of drugs, and I would say that all of this stuff was way more addicting than any of them. Back in the day when me and my partners were first playing around with generating tracks from

> phished accounts to cash at ATM, we had several trial and error periods, and the first time I actually heard the ATM clicking sound come on a money spit out (first successful trip) is a memory that I never will forget. This part sounds really sick, I still have dreams of going to the ATM to this day sometimes. Just the click sound and the money coming out....reminds me of that scene in Terminator 2 lol. I guess you could say that eventually the money became also addicting (and the just general ease of getting it) but overall I would say it's the "game" more than anything (NA-(F)CC-2).

The preceding discussion indicates, in personal terms, the increasingly professional nature of cybercrime offenders. But the professionalisation of cybercrime is also reflected in the way the business is carried out. As noted in the previous chapter, cybercrime has been growing in sophistication. The point US law enforcement agent Carter noted was the growing levels of automation, which has even led to online shopping experiences not dissimilar to legitimate enterprises (US-LE-2). Cybercriminals, like Roman Seleznev mentioned in the introduction, run virtual shopfronts where stolen credit card details among other goods can be purchased, just as one might buy shoes or clothing online. One simply enters the number of each product to be purchased and then checks out, making payment in an acceptable currency like bitcoin. No human interaction is required. Here is an example of one of Roman Seleznev's online portals where cards could be purchased:

Figure 1: Online Card Shop



Source: KrebsonSecurity

Cybercriminals have also adopted a number of other practices common to legitimate business. Krebs (2014, ch 4) outlines the surprisingly positive experiences some buyers have in purchasing pharmaceuticals advertised through spam. For instance, if a customer complaint is made, a refund is often promptly provided in order to avoid a chargeback from the bank in question. The malware business has also become increasingly sophisticated. As noted by Carter, one need not even sell or buy malware outright, but can effectively rent it instead (US-LE-2). This is because some malware firms manage their business just like a legitimate software company might. Instead of selling the product outright, they might license it to customers and build into the code a restriction that allows it to be used only for a certain period of time. They also have customer support that can be contacted if a user needs help using the product, along with those that effectively act as a marketing department ensuring strong sales for the

product (GER-CSP-1). Some more details of how these firms operate will be discussed in the final section. But for the purpose of this section, the key point is that these groups operate in ways that are highly professional and mirror many aspects of legitimate industry.

Markets

Markets are central to the successful functioning of an industry and the core of economic studies of the subject (Nightingale 1978). Marketplaces are distinct from markets, in that a market denotes exchange rather than a specific place to trade (Gravelle and Rees 2004, p. 3). Markets are "institutions that exist to facilitate exchange" (Coase 1988, p. 7). It should be clear from the previous chapter that marketplaces have played a vital role in the evolution of profit-driven cybercrime. They continue to play a key function today. Forums are highly visible and much literature focusses on them (Holt 2013b, Holt and Lampke 2010, Décary-Hétu and Dupont 2013, Hutchings and Holt 2015). Some books have even focussed largely on the stories of specific forums (Poulsen 2011, Glenny 2011). This creates the sense that large online marketplaces are the cybercriminal organisational structure *par excellence*.

But it is important not to overemphasise the importance of forums, rather than markets more generally, in the cybercriminal economy. They perform a significant role by providing a meeting place for those looking for partners to do business with, and provide a level of governance that improves the quality of that business. But there are downsides to involvement in forums as well, not least the greater exposure to

undercover agents and, even with the protections in place, being scammed by virtual strangers. In fact, law enforcement threats have weakened the effectiveness of these marketplaces and driven many to go further underground. In reality the cybercrime industry is much more complex than forums alone. This section aims to emphasise that there are a number of cybercriminals who do not involve themselves in major forums but are still able to operate and trade in other ways. Major marketplaces are not the only way in which exchange can take place. Instead, a more nuanced approach to forums is required, which views them as networking hubs within a much broader market and industry.

Major forums might be attractive to a number of cybercriminals, but there are also many who try not to involve themselves in that aspect of the business. As discussed in the previous chapter, some cybercriminals began to steer clear of major forums once law enforcement attention became too hot. In some ways, this trend has continued and smaller, more trusted, groupings have become a popular alternative. Chat groups are now making a comeback of sorts after the Golden Age of forums saw many cybercriminals favour those emerging marketplaces. But it is important to note that there are other actors who have not just moved away from forums, but have never involved themselves in large forums at all. Despite eschewing the key marketplaces, some of these actors have still managed to achieve success in their cybercriminal careers and make a good deal of money. For instance, Sean, who stole hundreds of thousands over the course of his career, explained it this way:

> I never got involved in the ShadowCrew side of things. I found that to be…there was more structure and business behind it. I didn't like it very much. That was more for the lower level carders. Whereas I was in a completely sort of different realm to

them. So I didn't get involved in that… (WE-(F)CC-1).

Dave, a talented hacker who has since gone legitimate as a pentester[29] but used to be involved in a spam operation, saw things in a similar way. Part of his resistance to joining major forums was that he believed that they were law enforcement stings. But, in addition, he preferred not to make connections with strangers on a forum:

> They wouldn't have the connections, which means they don't have the reputation, which means they haven't impressed someone. So it's pretty easy in the Internet, when you start getting good at anything in an illegal field, you start making friends and you impress people then get into those circles…
>
> …So I worked always with someone who came from a mutual recommendation, so someone else recommended them "this guy's good". So to meet some guy random on the internet, 'I don't know you from a bar of soap'. So no way" (SEA(E)-(F)CC-1).

There is a clear sense of superiority in these statements. In general, there seems to be somewhat of a hierarchy between different types of marketplaces and other groupings that have evolved. It appears that carding forums and others focussed more on the trade, cashing out and less technical aspects of cybercrime are "below" the more technical groupings that might focus on hacking or malware. These more technical forums may also have a stronger element of discussion rather than a pure business focus. Scott, a former North American cashout expert saw it this way. He was a relatively proficient hacker himself, but as noted eventually saw his interests would be best served by specialising on the money side, and effectively worked full-time on the activity. This is his outline of the unofficial hierarchy of forums: "The more "elite"

[29] An ethical hacker hired by organisations to test their security.

forums that I was on at that time were more of the hacking/malware/blackhat forums that mostly had alot of the people "above" the people on XXXX[30] and other carding forums at the time (they were suppliers to lower vendors etc on the carding forums)" (NA-(F)CC-2). Some even went as far as describing those on carding forums as the "stupid" cybercriminals who couldn't find a less risky way to make money (RUS-CSP-5, RUS-CSP-6). While there appears to be a technical divide and associated biases, I interviewed former cybercriminals involved with carding forums who nonetheless demonstrated high intelligence and/or strong technical abilities, even when some level of risk taking also seemed apparent.

Both Sean and Dave are instructive of how cybercriminals can successfully operate in an ecosystem not directly connected to the key marketplaces. Both were hackers on the technical end of cybercrime and had a deep interest in hacking in its own right, whereas a number of the large forums are more business focussed. As true hackers, both primarily operated in chat groups on various platforms. Dave referred to these as "social bubbles" (SEA(E)-(F)CC-1). Sean described the hacking groups he was involved with like this:

> Because it's just an open chat room it can mix between collaboration between projects – one of you is working on something and the other person sees and joins in. So it's very much open, there's no structure to it at all. You just do whatever the fuck you want whenever you want… (WE-(F)CC-1).

Despite not belonging to major trading forums, these two hackers also had no shortage of collaborators who could help them make money when they wanted to

[30] Forum name removed to maintain anonymity.

move in that direction. In short, other opportunities for exchange were available to them. They could still trade through the market, even if they did not frequent large online marketplaces. Dave usually relied on a mutual acquaintance to make the relevant introduction online (SEA(E)-(F)CC-1), whereas Sean was unusually self-sufficient. He sometimes partnered directly with his online acquaintances in a formal business relationship, but more often than not they were more of a collaborative technical support network. While specialising in taking over the bank accounts of victims, Sean never required the services of a cashout expert. He performed this role himself, recruiting those known to him in the local drug community (himself an addict at the time) to act as "drop girls" who would receive goods purchased with stolen funds (WE-(F)CC-1).

The cases of both Dave and Sean illustrate that cybercriminals can carry out exchange through less structured and visible channels. This is combined with the historical shift away from major forums that was outlined in the pervious chapter. Given this qualification, what role do large marketplaces actually play in the underground economy? Following on from this previous discussion, it appears that the key function of large forums is to provide a highly visible focal point for networking. This is why many cybercriminals are drawn to them. As noted by Script in the previous chapter, forums offer a location for cybercriminals to come together and meet others with specialties different from their own. They also offer a place for information sharing and learning. Fyodor, who was a member of CarderPlanet noted that Script actually required the forum's more senior members to actively educate the more junior cybercriminals in the ranks (EE-(F)CC-2).

The networking function of forums is apparent as much from those who participated in the marketplaces as from those who didn't. The stories of Sean and Dave above illustrate that if networking can be achieved through other means, whether through existing contacts, chat rooms, niche forums or offline contacts, then the major marketplaces are not essential for exchange. Scott also provided suggestions that many active forum users might be happy to recede from the marketplaces once they have sufficient partners and only return if their existing contacts disappear (NA-(F)CC-2). Of course, it is important to remember in such cases, that the forums are still important as the original source of contact between many of those who work together. In fact, CarderPlanet appears as influential for the creation of the first cybercriminal marketplace successful on a wide scale, as it is for the birth of a leading network of cybercriminals. This cohort continued to maintain ties after the death of that site and are often implicated in numerous high level attacks and schemes around the world (EE-(F)CC-2). As such, online marketplaces should be recognised as a significant aspect of the overall cybercriminal market. But it is far too simplistic to understand these marketplaces as the sole available means of exchange.

Firms

Cybercriminal forums are not organisations that orchestrate the activities of their members in a direct sense. They are in essence marketplaces. It is important to specify this, as it runs counter to the view put forward by a number of law enforcement agencies that paint cybercriminal forums as organisations with a clear focus and direction. For instance, the 2014 indictment of members of the Carder.su forum described matters in this way:

> The defendants herein, and others known and unknown, are members of, employed by, and associates of a criminal organization, hereafter referred to as "the Carder.su organization," whose members engage in acts of identity theft and financial fraud, including, but not limited to, acts involving trafficking in stolen means of identification; trafficking in, production and use of couterfeit identification documents; identity theft; trafficking in, production and use of unauthorized and counterfeit access devices; and bank fraud; and whose members interfere with interstate and foreign commerce through acts of identity theft and financial fraud. Members and associates of the Carder.su organization operate principally in Las Vegas, Nevada, and elsewhere.[31]

Given the difficulties in charging certain offenders, it is not surprising that the US authorities took such an approach in this case, even ascribing a geographical hub, Las Vegas, to a community that was spread across the globe. Classifying forums in such a way not only gives a sense of heightened harm but also makes them susceptible to prosecution under the Racketeer Influenced and Corrupt Organizations Act (RICO). This act has conventionally been applied to traditional organised crime groups and allows for more severe penalties for members of an ongoing criminal organisation.

But leaving aside legal imperatives, in organisational terms the activities of a forum's members are often quite distinct from the marketplace itself. While some forum officers may be held in high regard and may run successful money-making operations, this is theoretically separate from their activities managing the marketplace. There are also many others on these sites carrying out various cybercriminal scams. Many of these actors never serve as administrators, moderators or in other positions and some seem to avoid such roles as they may bring increased

[31] *US v. Roman Zolotarev and Others*, United States District Court, Nevada, 20012 [indictment].

responsibilities for what they see as little gain or unwanted attention from authorities (NA-(F)CC-2). Many members, sometimes numbering in the thousands, have not interacted directly with each other and often have little to no knowledge of the schemes that others are engaged with. Rather than joining to serve a well-structured criminal organisation with a clear goal, the central interest of forum members begins and ends with a desire to network, trade and engage in their own enterprises.

With regard to cybercrime, it's at this point that the concept of a firm becomes important. A *firm* is a business: a profit-making entity that supplies goods or services (Sullivan and Sheffrin 2003, p. 29). Coase (1937) famously argues that firms emerge because there are a number of costs associated with markets, not least obtaining the goods, information costs, bargaining costs and issues surrounding enforcement and trade secrets. In certain cases, production may be enhanced within a firm structure. Cybercriminal organisational structures are diverse, go well beyond forums alone and include a number of operational groupings that appear to approximate firms. The concept of a firm is what has been missing from much of the literature on cybercrime. Even though similar analyses have been applied to other forms of crime (Reuter 1983, Gambetta 1993), there has been too much focus on studying marketplaces rather than on those groups that actually carry out cybercriminal acts. These firms engage in cybercrime schemes, essentially production, rather than simply trading their loot. In fact, trade could hardly occur without this production. At the core of each firm is a boss, who is ostensibly a criminal technology entrepreneur, with the resources and organisational ability to employ the relevant talent. This leader is then supported by others with specialised roles.

The structure and roles within a firm will depend on the focus of the group. For instance, a firm focussed on actually deploying malware rather than developing it would appear different from the case described by Maksym in the previous chapter. In the case of a scheme involving a "trojan horse" that steals online banking credentials, the boss would first need to acquire the relevant malware, assuming he is not the original author/owner, and hire and coordinate a team of people who specialise in infecting computers with the malware to access the credentials. Of course, the process is not complete as the money still needs to be transferred out of the victims' accounts into accounts that are controlled by the criminals. After that, the funds need to be cashed out in some form, turning the virtual gains into physical ones and severing the money trail that leads back to the crime. The boss might employ people to carry out these latter functions, or else he might outsource to other firms specialising in these areas, or simply sell them the relevant products, such as compromised banking logins (UKR-CSP-1, UKR-CSP-3). These online groupings tend to be small and look something like a crew that might occur in other forms of crime, such as bank robbery. Each member of the group is brought in to perform a specific role.

Other firms appear to have a strong offline component. In the last chapter, this was discussed with regard to cash out crews and those directly engaged in carrying out the cybercrimes themselves, such as Albert Gonzales' operation. There was also evidence of "teams" built around geographical hubs in Eastern Europe, with a degree of longevity and involvement in multiple schemes over time (EE-(F)CC-2). These types of operational groupings appear to move beyond the idea of crews into something more substantial. Fyodor, a former Eastern European cybercriminal who operated at the highest levels, described these different teams as being built around some key

founders and a common geographical location. Such examples included the Odessa team, the Moscow team, the Donetsk team and the Sebastopol team. From Fyodor's descriptions, it appeared likely that some of the associates of these teams might have changed, but that the existence of the firms themselves lasted for many years in each case (EE-(F)CC-2).

Some offline firms are even more sophisticated in structure, appearing to move beyond crews to larger scale enterprises that approximate legitimate businesses. Like Fyodor's teams, the Carberp example discussed in the last chapter demonstrated how cybercriminals may operate out of fixed office space (Ragan 2012). On an even grander scale are enterprises like the Russian Business Network, which are effectively technology companies. They simply have more sinister motives. RBN was in reality an Internet service provider. Based in St Petersburg, it had an office and a number of employees. It just so happened that its core clientele were criminals and it would refuse to shutdown their hosting in return for a lucrative fee structure (Krebs 2014, Graham 2009). In Costa Rica, Liberty Reserve operated its virtual currency business in much a similar way to any other business, with the same exception that many of its customers were criminals.[32] Spam outfits based in Russia are ostensibly online marketing companies that engage in nefarious business practices to promote counterfeit pharmaceuticals among other products (Krebs 2014). A number of these enterprises can operate in the relative open because, like spam, they often fall within grey areas of the law within their country of operation. They often also make use of corrupt government agents and officials to shield their business operations for as long as they can. This aspect will be explored further in chapter 8.

[32] *US v. Liberty Reserve S.A. and Others*, United States District Court, Southern District of New York, 2013 [indictment].

There is ultimately no one universal group structure in cybercrime. There are numerous forms of cybercrime and the group structures are tailored to the activities in question. The purpose of the discussion above is to differentiate between what is the market for exchange between partners and what is the structure of groups that actually carry out various forms of cybercrime. It seems clear that these groups should be considered as firms, given the role that they play. But in certain cases, it may be difficult empirically to distinguish between very long term trading partners and members of the same firm. And while firms have become common, not every cybercriminal need be part of one. It is also the case that some lone wolves continue to persist, who operate alone and trade as their only form of interaction with other criminals. For instance, some of the leading coders who have been around for quite some time, may simply write the code on their own and, other than selling the product, may not be involved with collaborators in a significant way. These are some of the most cautious actors in the industry (UKR-CSP-1). These sole traders must feel that their interests are better served by not joining a firm.

Conclusion

This chapter has continued the argument that cybercrime is now a bona fide industry. In analytical terms, it operates according to foundational elements of industrial organisation that are regularly observed in other settings. There is a clear division of labour in cybercrime, with strong specialisation seeing different cybercriminals performing distinct functions. Cybercrime has also become increasingly professional, both in terms of the cybercriminals themselves and the way they conduct their

business. In addition, there is clear evidence for competitive markets. Large marketplaces play a key role as a focal point for networking and trade, but many other opportunities for exchange also exist. Finally, while often overlooked, there is strong support for the existence of cybercriminal firms. These groups serve as the primary drivers of production in the economy and are the lifeblood of the industry.

Thematically, there are two important issues that fall across these points. First, there is a significant, perhaps unexpected, offline dimension to cybercrime. Many aspects of the cybercrime industry surprisingly take place in the physical world. Exchange is not only possible online, but can also be conducted through offline networks. A number of firms are also rooted in the "real" world. In fact, this appears to be the case for the largest and most sophisticated cybercriminal firms, which begin to rival the size and structure of some larger licit enterprises. The importance of this offline dimension will be discussed further in chapter 7. The second key theme to note follows on from this point: geography is also very important to the cybercrime industry. This is particularly the case with regard to specialisation, but it impacts on how the industry functions more generally, whether in relation to professionalisation, markets or firms. Cybercrime is not a monolithic enterprise. The geographical background of offenders matters a great deal with regard to who they are, how they operate and even why they enter the industry in the first place. While this point is not specifically addressed again in this thesis, it underpins many discussions and should not be forgotten.

5. Nicknames and Identity

The last two chapters have examined how cybercrime has developed into a sophisticated profit-making industry. The focus of this chapter and the three chapters that follow is on how this development has been achieved given the key challenges faced by cybercriminals operating in a largely anonymous environment. How have they managed to collaborate, cooperate and organise to such a degree when they exist in a fundamentally distrustful environment? The subject of this chapter is a foundational problem for online criminals: identity. The introduction outlined the theoretical significance of trust and enforcement in enhancing cooperation. But in the context of online crime, there is no physical identity one can put trust in or seek enforcement against. Instead, nicknames become of fundamental importance. They become the central identity signal, without which one cannot operate in this environment. As Carter, an American law enforcement agent with significant undercover experience, put it: your nickname is "basically all that you have" (US-LE-2).

Cybercriminal nicknames appear to differ quite considerably from how aliases are used by conventional criminals and others. There is only a small literature on criminal nicknames thus far, but Maurer and Futrell (1982, p. 248) argue that criminal "monikers" have been around since the development of professional crime in fifteenth century Europe. Gambetta (2009a, ch 9) examined the phenomenon of aliases in the mafia, by looking at a sample of nicknames from Sicilian families. Varese (2001, Appendix A) extended this approach in relation to the Russian Mafia. In sociological

terms, these last two works likely go the furthest in delineating a typology for making sense of criminal nicknames (for other approaches see Zaitzow 1998, Black, Wilcox, and Platt 2014, Wilson 1997). This table summarises the key approach and is reproduced from Varese's appendix (itself adapted from previous work by Gambetta):

Table 3: Types of Aliases

	Source	Conferring mechanism	Motive	Content	Typical bearers
Nicknames	others	informal	expressive	mocking/ appreciative	Sicilian mafiosi
Code names	self/others	informal	instrumental	neutral	spies
Noms-de-guerre	self/others	informal	instrumental	neutral/ appreciative	partisans
Noms-de-plume	self	informal	expressive	appreciative	writers
'Second' name	self	formal	instrumental	appreciative	priests

Source: Varese 2001, p. 195

As this table summarises, code names such as those used by intelligence operatives and others, are primarily designed to hide identities and have no particular meaning in their choice. *Noms de guerre*, taken on by guerrillas and partisans, also have an element of secrecy and are designed to protect the identity of the bearer and their family. But unlike code names, a *nom de guerre* could become quite famous and could also have some meaning to the bearer if they so choose. Both Varese and Gambetta agree that nicknames are generally chosen by others, rather than the bearer and may involve a degree of fun. On the other hand, a *nom de plume* is chosen by the writer. Some may employ such a pseudonym out of personal preference, while others may have very specific reasons for doing so, such as writing politically sensitive

material in a dangerous climate. The choice of the name may have special meaning for the writer or it may operate like a code name, hiding their identity with little to connect them to it. Finally, Varese adds a new category to those originally considered by Gambetta: renaming. This is common among orthodox churches and secret societies when members join. The name is often chosen by the bearer, but is formally given by the institution. Perhaps the most famous renaming process is the one that occurs with the installation of a new pope (see Varese 2001, pp. 193-194, for more detail on these points).

In many instances, criminal nicknames appear to fit within the nickname category. Whether it is among gang members or mafia members, the names are often given by others and include an element of mischief. That said, they can also have some functional value, such as helping to distinguish between multiple characters with similar legal names or to shield real identities from law enforcement (Gambetta 2009a, pp. 239-246). But this does not appear to be a nickname's primary reason for being. There are other criminal groups that either don't use nicknames or use them in other ways. For instance, Varese's main finding was that *vory*[33] in the Russian Mafia approach aliases more as renaming. They adopt the new name as part of a ceremony where they become full members of the criminal fraternity (Varese 2001, pp. 195-197). This process appears to be much more ceremonial, symbolic and ritualistic rather than being a strategic choice that might protect members against law enforcement or other threats.

[33] A *vor v zakone*, or thief in law, is effectively a boss within the Russian Mafia.

Cybercriminal nicknames differ again from most other criminal aliases. They are not nicknames in the formal sense outlined above, because they are taken on by the bearer rather than given by others. Nonetheless, I continue to refer to them as nicknames because that is how they are commonly referred to within the cybercrime industry, or else as “niks” or “handles”. The chief function of a cybercriminal nickname is to protect the identity of the user, so they have more in common with code names, *noms de guerre* and *noms de plume*. But such nicknames differ even from these categories in that they extend beyond simply covering one’s true identity. They function as an identity signal for the user’s online existence. Without such a handle, they can't operate at all. As we shall see below, in some sense it becomes a bona fide second identity, often even with a different persona from that of the offline user. A writer might adopt a *nom de plume* to publish works, but they will rarely communicate and collaborate extensively with others under this alias. They would rarely develop a functional second identity. For cybercriminals, such an identity is essential for carrying out business online. If any categorisation fits how cybercriminal nicknames operate within the industry, it is perhaps the concept of a *brand*. This is discussed in the following section.

This chapter examines how nicknames are used by cybercriminals to build an identity online and the challenges they face therein. Building an identity can be a complex and unstable process, given that nicknames can be altered far more easily than physical identities. This chapter addresses a number of points of interest in this regard. First, it investigates the manner in which nicknames act as online brands for cybercriminals, as well as their possible appropriation/manipulation. The second section examines how cybercriminals choose these specific brand names and whether they are

inherently meaningful. The third section follows on by determining whether nicknames can be successfully interpreted to provide some detail about the user behind them. The final section investigates the central tension with regard to nicknames: that anonymity is both a benefit and a cost to cybercriminals. Cybercriminals cannot operate without an identity signal, yet they must still attempt to protect themselves with as many name variations as they can afford. They cannot completely abandon their identity, as this would waste the reputation they have developed; yet their reputation is the very thing that can incriminate them or put them in danger with other criminals. This section explores how cybercriminals attempt to manage this challenge with their nickname strategies.

Nicknames as Brands

Nicknames effectively act as brands for many cybercriminals. Each handle is the foundation of a cybercriminal's reputation; without it he has no presence in the online market. If, for instance, a cybercriminal builds a reputation as a trusted vendor of a certain type of illicit goods, he must maintain the same nickname to benefit from that reputation. If the cybercriminal starts using a different *nik* to sell his wares, all the goodwill he has accrued would be lost and a new reputation must be built from scratch, with the associated costs of loss of business. This idea of a brand was confirmed by a number of former cybercriminals and hackers whom I interviewed (WE-(F)H-1, NA-(F)CC-2, EE-(F)CC-2). Sean believed "nicknames not only act as a sense of reputation and identity, but depending on your reputation also acts as a medal of what your rank is within the hacking community" (WE-(F)CC-1). Former leading Eastern European cybercriminal Fyodor saw matters in this way, writing:

> for many nickname is a "brand", so when you choose it, it means a lot. It is even more so, if one elects to promote his services or sell proceeds of his activity. In such case his fame, reputation and standing relation is all dependent on his nickname (EE-(F)CC-2).

But given one's true identity is not linked to the nickname, this branding operates in some potentially unstable ways. First, individuals can choose to operate more than one nickname to control more than one brand. This might be the case with vendors in particular, whose business is to sell products as best they can. Part of maintaining several brands is linked to diversifying risk should a particular nickname be tarnished, which will be discussed in the final section of this chapter. But it is also used as part of standard business practices. For instance, a cybercriminal might have two separate businesses that provide distinct services under different nicknames. In the Carder.su forum there was a user who went by the names Bank Manager and Document Manager in order to advertise his various services.[34]

Another reason to maintain multiple brands might be less honourable: a means to offer the same products at different prices. For instance, Scott knew of one leading card data vendor that sold his wares through his own site. But Scott later found out that this cybercriminal had started a new "reseller" site under a different nickname: "but really it was in fact the same exact person on the backside of it, it was just a way that he could raise his prices to all the newcomers etc" (NA-(F)CC-2). It appears that he could charge higher prices on this second site, by closing the first site to new members, unless they were invited. In a sense, he was maintaining his existing

[34] *US v. Roman Zolotarev and Others*, United States District Court, Nevada, 20012 [indictment].

clientele and then seeking to expand his market by profiting from less discerning, and perhaps less experienced buyers, who did not have the pre-existing relationships to purchase data at lower prices. He could do this without raising much suspicion, because it is quite common for "dumps"[35] vendors to have resellers (NA-(F)CC-2). But in these cases, the extra cost might be expected to result from the need for the resellers to make some money for themselves. This example shows an attempt to appropriate that explanation as an excuse to gain higher profits for the original seller.

Second, not only are there individual cybercriminals with multiple handles, but there are also reverse cases of multiple users making use of the same nickname. Some of these cases might make use of one core brand and have related nicknames to indicate support staff, such as XXXX Support. This would be an employee of the central nickname XXXX. Such employee support nicknames were particularly important in the past, before automated shop fronts dominated the business, as the support staff may have been manually required to take orders when the main player was offline (NA-(F)CC-2). Others might make use of the same exact nickname. Trusted friends may share a login because one cannot be bothered attaining entry into a forum or might struggle to be vouched in if it is closed access. In other cases the nickname might serve as the brand for an entire team working behind it (NA-(F)CC-2). While not necessarily malevolent uses of the same nickname, these instances demonstrate the difficulties in ascertaining true identities when dealing with online actors.

Finally, linked to these issues, there are a number of opportunities for: confusions over genuine identities; nicknames to be hijacked; and other manipulations to take

[35] *Dumps* are card details stolen from hacked point of sales systems.

place in this online environment. Some mix-ups happen because certain nicknames are common, such as John Dillinger or Frank Abagnale (NA-(F)CC-2). It is also common for nicknames to be influenced by the pop culture of the time. Following the release of *The Matrix*, a number of users called themselves Neo or other names related to the movie (NA-(F)CC-1). As will be discussed in the next section, many cybercriminals will actively try and choose a name that is not commonly used to avoid this type of confusion. This allows them to establish their own brand.

But sometimes the opposite approach is taken. For instance, elite hacker and forum administrator Max Butler chose the name Iceman to administer CardersMarket precisely because it was not original. There were already other Icemen floating around the online underground. Butler's logic was that if he ever attracted heat from law enforcement, these other users might complicate efforts to identify him (Poulsen 2011, p. 127). Others have taken a more nefarious approach, actively trying to impersonate other users to appropriate the benefits of their reputation. This is sometimes the case when the cybercriminal in question has retired or been arrested and is no longer in a position to contest the brand (NA-(F)CC-2, EE-(F)CC-2). It should also be noted that such a strategy is risky and most likely for short-term gain because, if the ruse becomes apparent, the user will appear untrustworthy in future dealings. It is also not too difficult for old partners to seek verification through closely examining the user's wares, requesting the use of old chat accounts or emails that they know belonged to the user or by asking specific questions that only the true identity would know the answer to (NA-(F)CC-2). These issues will be discussed further in the next chapter.

Of course, criminals are not the only ones who impersonate other users through their nicknames. This has also been a tactic of law enforcement. In one early case, a (now former) US law enforcement agent, Landon, was involved in the arrest of a major cybercriminal. But only a short time later, his network of informants began to report that the nickname was active online once more. Landon investigated and felt that the nickname's use exhibited law enforcement traits, suspecting that it was being used by a different agency for its own purposes. He tracked down the agents involved and instructed them that they were jeopardising the case, as the defence could claim that the nickname had always been operated by law enforcement rather than the arrested suspect (US-(F)LE-8). In other cases, nicknames can be purchased and then used by law enforcement or others, effectively buying the reputation and access tied to that name. But perhaps more dangerous is when cybercriminals are leveraged into turning informant for law enforcement, as no impersonation has to take place. They already own the brand and know how to operate it. This appears to be a key weakness in the safe management of nicknames.

Choosing Nicknames

While cybercriminal nicknames may act as a brand, a choice still remains as to how to best name that brand. Choosing handles is more of an art than a science. There do not appear to be any clear rules, but certain core principles are apparent. The most fundamental of these is not to use your real name or any other details that might be linked back to your offline identity. This is very much tied to protection from arrest or other harm. As Noah put it: "I don't want these guys to know who I am and they don't want me to know them. If you get arrested you can tell on them" (NA-(F)CC-1). Not

using one's real name might appear obvious, but in the earlier days of cybercrime, when concerns about law enforcement were lower, a number of users made mistakes in this regard. Fyodor used part of his real name when he began in the business, but later realised this was "stupid" and changed it (EE-(F)CC-2). In the days of Counterfeit Library, Lance actively counselled other users not to use *niks* linked to their real identities in anyway, such as middle names (NA-(F)CC-3). In later periods, it has been less common to see people using nicknames associated with their true identities, but there are still cases. For instance, the real name of the leading Ukrainian carding vendor Maksik is Maksim Yastremskiy (Zetter 2010), while SMI was the online alias of the Russian Dmitry Smilyanets (EE-(F)CC-2). Even without direct nickname connections, thorough investigations can sometimes trace back links between nicknames, logins, email addresses and other digital footprints that might begin with a younger more naive user who did not take operational security into mind.

Assuming that one abides by the golden rule, and that their nickname is not their real name, the specific choice appears to be a very personal one. As noted above, popular culture plays an important role in some choices, with movies a regularly noted form of inspiration. Veteran carder and film buff David Thomas used the online nickname El Mariachi as a tribute to the Robert Rodriguez film (Zetter 2007a). Various mythological gods and figures are another common source (WE-(F)CC-2, EE-(F)CC-2). Robert Schifreen, the former British hacker whose early hobby exploits partly led to the introduction of the United Kingdom's Computer Misuse Act in 1990, went even further my naming himself Triludan the Warrior after the anti-histamine medication he used (Lusthaus 2013a). On the whole, many appear to choose names based on whatever "sounds cool at the moment" (NA-(F)CC-1).

But, ultimately, the nickname effectively becomes an online persona. It should be something the cybercriminal in question likes and feels that they are well represented by:

> As to the significance of nickname, for each person it is his own. For me, as for many others, it is like short description of your alter ego, whatever you want it to be, behind the screen, because very often, your nickname is what people on the other side know first of you, it's your first impression on them (EE-(F)CC-2).

In Fyodor's case, his key driver was to produce something "short" and "crisp", which he felt best reflected his persona (EE-(F)CC-2). While he had some technical ability, he did not view himself primarily as a hacker and thus did not choose a nickname that reflected that. In some instances, the reverse happens and cybercriminals appear to take on the personality traits of their nickname. Poulsen notes how Max Butler actually altered his online behaviour according to the roles he was playing and the identities he had taken on. For instance, as the administrator Iceman, Max would be cool, ruthless and aggressive – a contrast to his real personality, which was more affable and subdued (Poulsen 2011). This resonates with the broader idea that people are able to create a new persona for themselves online, which parallels clichés of Internet dating among other online interactions.

The element of randomness in some nickname choices can be taken to the extreme. Dave originally had no attachment at all to the nickname that he chose:

> I picked a random name out of the dictionary and I always stuck with that name. The best advice I had from someone was

> when I was probably about 15 on the Internet was he told me: have one name and use it and get a reputation. Okay, alright, so I got this alias and there are still people that I used to work with when I was cracking software when I was really young and I still talk to them. I am still,…with that alias, and they know me and they have the same alias, they now have three like kids, and they're still doing it. But I guess can't stop. I just picked a name out of a dictionary, completely randomly. No attachment. But later I found out that the word was actually quite cool and I kind of liked it a lot, *it's a cool word* (SEA(E)-(F)CC-1).

Other names are much more functional, their choice far from random. As noted above in examples like Document Manager, some names might be specifically linked to the business service on offer. Another would be Track2, connected to the magstripe on cards, which was the handle that Roman Seleznev used to sell *dumps*.[36] In other cases the functionality is less specific. For instance, while Max Butler chose Iceman to be the enforcer and leader of a criminal market, he used Generous and Digits for his personal vending of card data, implying positive dealings and attractive profits in each case (Poulsen 2011). In yet other cases, there is a strategic calculation in the choice of name. Albert Gonzales, the Cuban-American hacker and Secret Service informant who helped bring down the forum Shadowcrew, originally went by Cumbajohny and Soupnazi for different purposes, but later rebranded himself as Segvec and built a new persona as a leading Ukrainian black hat hacker. This was perhaps to shield his true identity but perhaps also to caplitalise on the good reputation of Eastern European suppliers (Verini 2010). This leads us to the next section discussing whether the interpretation of nicknames can provide any insights into the true nature of the people behind them.

[36] *US v. Roman Zolotarev and Others*, United States District Court, Nevada, 20012 [indictment].

Interpreting Nicknames

The previous section indicated that the key importance of a nickname is twofold: to shield the true identity of users and to build a distinct online brand. A successful brand can be built on even a random choice of handle. But in many cases, cybercriminals have some reason for choosing their specific nickname, even if it is not a particularly significant one. Nonetheless, some believe this choice can be interpreted to offer clues about a user's true identity. As Fyodor wrote:

> More sophisticated nickname is, more sophisticated it's author. It is clear that individual have to give some though to his nick(and if he did not, you can tell it right away), and so, sometimes it is like a crypto with his thoughts he gave it, which are to decrypt - more layers, more sophisticated person or his activities is. Choosing a nickname, is somehow, like naming children. What you can tell from the name? If you use similar approach to nicknames, you will understand more (EE-(F)CC-2).

The collected data suggests that nicknames might indeed be interpreted to reveal age/experience, technical ability and national, linguistic or regional backgrounds. First, a number of interview subjects suggested that the age and relative experience of users can sometimes be determined from their nicknames (WE-(F)CC-1, NA-(F)CC-2, EE-(F)CC-2). The key identifiers are long and excessively complex handles. As Sean put it:

> You can modify it like either reverse it or you could add different characters to it or you could put things in star key, decorating it essentially changing it. Usually what happens is, the more elaborate the nickname the more nubey the person is. Your nickname starts to shrink down and simplify over the years. So mine started off as a ridiculously long one with decorations off the front and a star and now it is just four

> characters. The sign is when someone has a smaller nickname not bothering with upper case lower case, it shows they are more grown up, which is very strange. It is not an exact science, but it usually shows what mindset that person currently has (WE-(F)CC-1).

It appears that over time more experienced operators employ the confident understatement and ease of use of much shorter simpler handles. For Noah, who also began hacking as a teenager, after two years he found his original nickname "was just too long. So I abbreviated it just like you would John, being called John" (NA-(F)CC-1).

Second, some aspects of technical ability might be derived from a nickname. As Fyodor wrote:

> For "carders"(this is a slang name for cybercrimnals who specialize in credit card fraud), who primarily have more computer-related speciality(and skills), selection of nickname is deeply rooted in cyberpunk culture, not unlike hackers. Black hat hackers, who turned to commit credit card fraud, elected to do so because of lucrativity and simplicity of this business, comparable to other "areas" of for-proffit black hat hacking, but in context of this discussion on nicknames, it is worth notice, that sometimes(but not always) is relatively simple to identify "carders" with such a hacking background. On other hand, those who do not really have "undeground computer culture" background, you can also spot by lack of "sophistication" to their "nick"… (EE-(F)CC-2).

The key idea here is that a nickname would reflect some technical knowledge that may not be known by the average user, who does not have the interest or experience in the relevant subject area. For instance, Fyodor analysed the nickname sp0raw to demonstrate the knowledge involved, suggesting it was a "smart nickname derived

from assembly language, presuming tricky operation with sp registry". He argued that from this nickname you could tell that the person who made up the name: "a) knows assembly language; b) familiar with disassembler's and it's tricky workarounds; c) most likely has disassembling skills, and therefore, given context I heard this one, I may(not even knowing more) suggest that most likely this person has to do with malware". Other names implying technical knowledge could be Segvec, which is a "non-standard array type descriptor in one of C++ libraries(I may be wrong, but it's along with, along with ::vector, ::segment and ::stdmap etc descriptors)" (EE-(F)CC-2).

Finally, nicknames might also be useful in determining the national, regional or linguistic backgrounds of certain individuals. English language names and references to Western pop culture, might suggest the user is from such a background. Meanwhile it is common for some cybercriminals to spell out Russian words with the Latin alphabet, such as Graf, Deputat. Graf is an aristocratic title (earl/count), while Deputat is deputy - a position of political authority. In both cases they imply power and a form of protection (NA-(F)CC-2). But, of course, a little knowledge of Russian or the use of Google Translate would not prevent the choice of such names by non-Russian speakers. But other names require a greater knowledge of the Russian language and Eastern European cultures. As Fyodor explained, the name ncux (another handle of Roman Seleznev) provides an interesting illustration. It could be dismissed as somewhat random by English speakers, but when read according to the Cyrillic alphabet rather than the Latin letters, it spells out псих, which means psycho (EE-(F)CC-2). This is suggestive of a Russian speaker behind the nickname (it should be noted that some of Seleznev's other names, like Track2, are in English). With another

example, Fyodor went further to suggest cultural references might also be suggestive of the user's background. He wrote:

> "Borman" is likely to be character in popular soviet movie(as well as subject of many jokes), portrayed after Nazi Bormann, therefore, I can conclude that bearer of that nickname is either neo-Nazi or of Soviet origins, second thing likely, since Westerners doesn't often bother themselves with such a study of history, and it is not likely that somebody in the Britain or US studied about Bormann outside college (EE-(F)CC-2).

Fyodor acknowledged that his method of interpretation was not perfectly accurate, but believed that, even subconsciously, these elements might give a feel for the user and whether you might like them or not (EE-(F)CC-2).

While the indications of age seem tied to exuberance and overstatement on the part of inexperienced users, the suggestions of technical or national/regional/linguistic backgrounds are connected to something deeper. In this case, the interpretation is linked to some degree of investment being required. In order to choose those names in the first place, you must have some experience or knowledge of certain topics. To choose the name sp0raw likely requires a knowledge of assembly language, which suggests time spent on this endeavour. The names ncux or Borman require at least some linguistic or cultural knowledge from a specific region. This means that the person has either grown up in that region or actively sought knowledge of it. The nicknames that would better indicate someone from a specific background would be those that require extensive knowledge of that background. The more specific the reference, the more difficult for the nickname to be appropriated by someone of a different background, whether for "nefarious" purposes or otherwise. It's beyond the

scope of this chapter, but this aspect of cybercriminal nicknames would likely be well suited to analysis through a signaling theory framework (see Gambetta 2009b, Spence 1973, Zahavi 1975).

Balancing Anonymity with Identity

While the issues of branding, handle choice and interpretation are very important, there is perhaps a more fundamental point at the heart of this subject of nicknames. As noted above, the primary requirement of an effective handle is that it provide anonymity and cannot easily be used to identify the cybercriminal in question. It is the feature that, in effect, allows cybercriminals to advertise their criminality openly online. But one irony of the online underground economy is that anonymity is as much a challenge as a benefit. On the Internet, you begin with no identity whatsoever. Cybercriminals must construct an identity and attempt to reduce their anonymity in order to build a brand and attract criminal partners. But this can only be done to a point where they remain disguised to law enforcement and without becoming vulnerable to other criminals who may wish to do them harm. What cybercriminals attempt to do is to pierce the veil of anonymity that the Internet affords them, but not to discard it entirely.

This leads to the central tension of cybercriminal nicknames. On one hand there is an incentive to maintain the same *nik* or a variation of it over time. On the other hand, there is a competing incentive for cybercriminals to change online names regularly in order to distance themselves from past crimes, should they ever attract the attention of the law, or misdeeds against other cybercriminals. A calculation must be made as to

what approach to take. Rather than one equilibrium forming, there appear to be a number of approaches cybercriminals take to address this tension. These likely depend on their personal circumstances and preferences: 1) some use particular nicknames for different aspects of their business, or regularly change nicknames over time, in order to spread/reduce risk; 2) at the other extreme, there can be a tendency to maintain one or as few names as possible by those who treasure their reputation over any risk that it brings; 3) finally, some users appear to engage in a midway approach, hedging between these two extremes.

With regard to the first point, there are those who maintain a number of different handles or change them regularly in order to protect themselves. While not the most extreme case, Max Butler operated a number of handles for particular purposes, including Ghost23, Generous, Iceman, Digits and finally Aphex. His story offers an interesting example of nickname strategies, an account of which is found in Kevin Poulsen's *Kingpin* (Poulsen 2011). The first two names he used respectively in the pirating scene and early in his career as a forum vendor of hacked credit card details. As noted above, Iceman was chosen as Butler's administrator nickname as it was sufficiently common to perhaps subvert law enforcement investigations. But Butler also operated another nickname on CardersMarket, Digits, which he used to vend his stolen credit card details. The thinking behind the two different handles was another strategic decision: if the heat ever came, Iceman could claim to be running an informational website, which Butler did not believe was illegal. Only Digits would go down and Iceman and CardersMarket would remain. Butler was essentially diversifying his risk. But when the heat came for Iceman, he simply retired the handle. After starting a cyber turf war with DarkMarket, attracting media attention

and (ironically, in hindsight) making unproven accusations that Master Splyntr was actually a "Fed", Butler decided Iceman's reputation had become too damaged to continue. Instead, Butler as Aphex became the new leader of CardersMarket.

This example demonstrates the different ways that nicknames can be employed to address the tension of maintaining a brand, while reducing the risks associated with it. Particular nicknames might be used to operate distinct brands and spread risk between them. This attempts to quarantine some online activities from others, such as selling credit data from administering a forum. This also perhaps reduces the appearance of conflicts of interest, but paradoxically may also allow an actor to perform the role of judge in cases involving his/her business. In other cases, users might have multiple nicknames, using certain *niks* for different groups they were associated with, rather than within them. Noah had observed this approach and believed it was a good way to spread risk. He suggested that if hackers employ multiple nicknames they may keep them separate: "so this group of people knows me by this name, this group knows me by this name, the idea being that if this group ever got taken down they wouldn't be able to trace your activity to this other group because they all know you as something completely different" (NA-(F)CC-1).

Nicknames may also be dropped and changed to new ones if they have become tarnished. In Butler's case, a new name was chosen in response to specific developments. In less dramatic circumstances, Noah suggested that handles might be abandoned if one had simply moved on and didn't want to be associated with particular activities anymore (NA-(F)CC-1). But some cybercriminals also regularly change their names as a matter of operational security. Carter a US law enforcement

agent with extensive undercover experience online had observed this directly: "I know certain Russian malware writers that change their nickname about every three months. I look back at the last 5 years and they probably have 20 different nicknames we've been able to connect to one another" (US-LE-2). Fyodor supported this view, but noted that it was a relatively new development. In the past it was common for users to take great pains to develop a nickname and well-rounded "alter ego". But that trend is now "slipping away". He suggested that the "younger generation" was now much more likely to care little about the handles that they use and to change them often in the face of security concerns (EE-(F)CC-2).

This leads to the second point concerning cybercriminals who choose to maintain one name for lengthy periods of time. In the example of Dave noted above, where he chose a nickname randomly out of a dictionary and then kept that same name over time, the clear decision was to maintain a brand over any concerns of risk. This was despite the "real catch" that "if you google it, there's all sorts of stuff associated to it. So it sticks". Dave explained his reasoning for not changing names in order to protect himself:

> But then you'd have to start from scratch. It's like changing a real name. If you were no longer Jonathan and you are now known as Bob… haha. You've got to start from scratch, it's not worth it. I mean I've got a reputation, I've got friends, people trust me, I've got a good working relationship with many people, and I like that. So no, I wouldn't change it.

Now that he has moved into the legitimate security industry, there might be a threat of people finding out his past. But even this hasn't been a great concern for Dave: "To be honest, people have, clients have and they like it. They think that's awesome.

You'll do an even better job because they know you are really fucking going for it" (SEA(E)-(F)CC-1).

Part of Dave's approach could be viewed in the context of beginning his on-and-off cybercriminal career when law enforcement was not as active in this space. The risks were simply lower, even only as far back as last decade. Yet, while they are now less common, such practices still continue. In fact, there appear to be certain roles within the cybercrime industry that encourage the use of one name for as long as possible. While Carter noted that Russian malware writers change names regularly, it may be that their role in the industry allows this. Such actors often work in smaller groups, or even alone, and the cautious ones will only deal with people whom they know relatively well. As such it is much easier for them to keep their key contacts aware of any nickname changes. The high value of their services in the market allows them to keep a low profile. On the other hand, there are other types of cybercriminals who benefit from using the same name over time. These actors perform functions that require them to interact with a large number of other users, some perhaps whom they have not dealt with before. Foremost among these are vendors. Scott argued that someone who changed their name regularly as a matter of routine procedure was often "someone more behind the scenes", who might for instance provide "dumps" to vendors who then sold them on in smaller amounts. But it was rare for someone with a ""brand name" that they relied for vending" doing this. Scott wrote his summation like this:

> I would say this is more a problem for the people that depend on the "brand name" much more, such as vendors etc. It would be allot easier for someone on the hacking/cashing/buying side of the business to change nicks if he had already established

> contacts etc. This is one reason most of the hackers stealing most of the data sell in bulk to the vendors that have the brand. They don't want to expose themselves to so much heat that the vendors already do (because they cant really change nicks etc) so they sell in bulk to the vendors (with the already established brand names) and let them piece them out (NA-(F)CC-2).

In some sense, the high level suppliers are effectively selling unwanted risk along with the goods they provide. The vendors buy the risk because they otherwise can't access the product. This point further compounds the view that cybercriminals are not monolithic. There are many specialised roles within the industry and it is not reasonable to expect they all operate in the same way.

Third, few cybercriminals actually fall at either extreme of changing nicknames very regularly and not leaving a trail, or keeping just one handle for their entire career. Many fall somewhere in between, hedging between maintaining one name and multiple names. There are two key strategies employed here. The first involves cybercriminals leaving a clear trail between their new and old nicknames. Some might talk openly on boards, introducing themselves as one handle aka another *nik* that they are/were known by on other boards or channels:

> Your nicknames kind of follow you so what usually happens if you introduce yourself as someone, you'll join a channel with a usual nickname and then they might say aka Nick1 Nick2 Nick3 blah blah blah blah blah. So you kind of take a trail of these nicknames with you and you do use them to show people your reputation within the hacking community. And it can also work vice versa, if someone says I am affiliated with this this this person or I was known as this this and this, and that person says never heard of them then you know that that they are probably not really, well they are either from a different hacking group that you don't want to be part of or they're just a nube and you know to stay away from them (WE-(F)CC-1).

Others might be more secretive about it and only alert trusted partners to their new or different identities. But in many cases, some link has to be made or their original reputation will be lost entirely, even to their close associates (NA-(F)CC-1). While he had noted some cybercriminals change their nicknames very regularly, Carter also suggested that such links still needed to be made in that case (US-LE-2). Without cybercriminals letting others in on their nickname change, their associated reputations would disappear.

Of course, there must be ways to signal credibly that you are the same person behind previous nicknames. But care must also be taken that the trail is not so obvious to everyone that the nickname change is rendered pointless. Scott wrote a summation of how this works:

> If you were to change nicknames and still wanted a select few people to know it was the same person, there are a few ways someone can tell its you or not. Alot of people will first check to see if the person is on the same ICQ/Jabber/email account (or has the ability to login to the old one still) and then will ask a verification question like I talked about before. Some people choose that drop the name and start all the way over, maybe sometimes later on confirming that it is the same only to a few people they trust really well. If you are a big ripper then they would most likely not reveal that because word travels etc (NA-(F)CC-2).

This also raises a related issue of importance: that online identities can be confirmed through other technical markers. In this case, Scott mentions the ability to log into known accounts. Fyodor attempted to use "supercookies" to determine if a machine was the same one. In basic terms a *supercookie* is, like a cookie, a small piece of data

stored in a user's browser so that it might be recognised by a website in the future. What makes a *supercookie* special is that it can't be removed as simply as a regular cookie can by clearing one's browser. In his communications, Fyodor described it as the: "digital fingerprint of a client's machine derived from such a subtle settings as screen resolution, installed software, language configuration, regional settings or even very specific font sizes or flash, JavaScript, java vm settings, which are very specific for each machine. Thus, there several algorithms, which could tell you possibility that it is the same machine, whether client reset it's configuration or not" (EE-(F)CC-2).

The second hedging strategy involves maintaining the same core nickname but varying it over time. One alters the name multiple times but maintains a similar strain throughout, so that there is a connection between the variations. As above, Sean's nickname started out very long and decorated and shrank down to just four letters. But the core of the name was the same. Casper approached matters in a similar way. He took a core part of his name and then changed the consonants at the front of it to create different words over time, but maintained the essence of the name (WE-(F)CC-2). Both Sean and Casper were young hackers, who may have made some online choices based on fun rather than pure strategy. In Casper's case, he also had somewhat limited dealings with for-profit activities. Among older offenders who are more directly engaged in cybercrime as a profession, this approach of varying one name over time appears more rarely (NA-(F)CC-4). Managing multiple distinct names appeared to be a much more common hedging strategy instead.

Conclusion

While nicknames may be an interesting curiosity in relation to conventional criminals, within the industry of cybercrime they are of utmost importance. One cannot exist online without an identity. Online handles solve this problem to a degree but also lead to a number of complications and paradoxes. This chapter suggests that anonymity presents a number of ironic challenges for cybercriminals. Online criminals cannot operate without an established identity, yet they must still attempt to protect themselves with as many name variations as they can afford. The reputations that allow them to operate on the Internet are the very things that can incriminate them. Anonymity can hide online criminals from law enforcement but makes it harder for them to determine which other users might be undercover agents. It can protect cybercriminals from the violence of other criminals, but offers little recourse to enforce agreements with untrustworthy partners without the traditional underworld option of "paying a visit". In short, anonymity on the Internet is not necessarily (or even primarily) a boon to cybercriminals. It brings with it great costs and leads them into a series of games to address this challenge of identifying those they wish to deal with, and those they want to remain distant from.

This chapter has outlined the various ways in which cybercriminals attempt to overcome these obstacles. It illustrated how nicknames act as online brands; how specific nicknames are chosen by cybercriminals; means by which nicknames can be interpreted to provide background on true identities; and finally it examined the ways in which cybercriminals must balance the need for establishing a brand to conduct business, with the need to maintain a low profile and distance themselves from past

actions. Ultimately, cybercriminals manage these challenges as best they can. They must be able to establish functional reputations through their nicknames. While they act cautiously in this regard and sometimes forgo the value of the reputations they have built, without the ability of nicknames to establish brands online, cybercriminal cooperation would be next to impossible. The entire illicit industry online would collapse.

6. How Cybercriminals Cooperate Online

The previous chapter examined how cybercriminals establish and manage an identity (or multiple identities) in an online environment. This is of vital importance to cooperating with other cybercriminals. Without an identity, there is no vessel to put trust in and there is no entity with which to enforce agreements. While online identities remain somewhat flimsy and unstable in relation to physical identities, the ability to maintain some form of brand is a prerequisite for collaboration to take place. Once cybercriminals have a brand to work with, the next step is determining how they actually cooperate with each other. Great distrust still remains in their online environment, because all potential partners are either anonymous criminals or, worse, undercover agents. Earlier chapters have argued that cybercrime is now an industry. But such an industry requires relatively high levels of cooperation. This chapter examines what mechanisms have been developed online that allow this cooperation to take place in such a low trust environment.

This chapter draws heavily on aspects of the theory outlined in the introduction. The first section investigates the importance of trustworthiness for cybercriminals online. The second section discusses the other key element that might conceivably lead to increased cooperation: enforcement. The third section assesses how the lucrative rewards of cybercrime might encourage collaboration because some of the risks involved are outweighed. The final section allows for some variation and considers instances of where cooperation is less successful among cybercriminals, and what

these cases can teach us about the likely mechanisms that lead to more effective collaboration.

Trustworthiness

As noted in the introduction, it is trustworthiness rather than trust that is a core element in enhancing cooperation. Trust is essentially the risk one is willing to take on in a transaction, but higher levels of trustworthiness in partners will reduce that risk and make cooperation more likely. Following Sztompka (1999), this section breaks down the discussion of trustworthiness into three key components: reputation, appearance, performance. It deals with each in turn.

Reputation

From a number of the interviews I conducted, it became clear that reputation plays a very important role among cybercriminals (SEA(E)-(F)CC-1, US-LE-2, US(E)-CSP-1). It is more significant than any of the mechanisms to be discussed below. As one senior security firm officer and former hacker put it: the "whole world revolves around reputation, everything revolves around reputation" (UK-CSP-1). Former spammer Dave, who mixed with the more technical layer of cybercrime and stayed away from major forums, explained the importance of reputation:

> …most of these guys, it's small circles of friends. Little groups all like associates. That's why I said at the beginning like reputation. So if your reputation gets tarnished and you get pushed out of your little bubble, word spreads pretty fast among the other little bubbles close to your bubble. Like you tell your friends, your friends tell your other friends oh that

> guy he fucking ripped me off, he's no good. So then you're working with, instead of the higher caliber people who are dealing with large sums of money then they would probably have to work with like Nigerians or, I don't know, someone who doesn't have that much cash. It wouldn't be worth it (SEA(E)-(F)CC-1).

But, as discussed in the previous chapter, online reputation is tied to nicknames rather than a physical identity. In terms of reputation, these handles effectively operate as brands for cybercriminals trying to participate in the market. Bearing in mind the instability of reputation in the world of cybercrime, this section will address the key elements that became apparent through the collected data: 1) the importance of repeated interaction; 2) the regular use of referrals and background checks by cybercriminals; 3) the way in which forums institutionalise the reputation mechanism and scale its usability to thousands of members.

As noted in the introduction, repeated interaction is a cornerstone of building reputation in a number of social interactions (see Axelrod 2006, Klein and Leffler 1981, Abreu 1988), so it is unsurprising that it would be equally important to cybercrime. If two cybercriminals interact with each other on a regular basis, it is not difficult to see how this might build familiarity and ultimately reduce the perceived risks of doing business together. This could be due to parties being able to test incrementally a partner's ability and willingness to carry out their side of the bargain. In addition, over the course of this relationship each side can sanction the other for defections, perhaps leading to greater compliance. On the other hand, repeated interaction itself may actually incentivise cooperation over the course of dealing. Schelling (1980, pp. 134-135) argues that trust can be achieved because parties may

recognise they have more to gain from a "tradition of trust" than from cheating in one instance.

Phillip, a former UK law enforcement agent, provided an example of how those employing "money mules"[37] to transfer the proceeds of a cybercrime might benefit from repeated interactions:

> [W]hat would happen is that they would put an advert up on one of the sites and say, 'I need a money mule to transfer money between the UK and Russia.' So people would volunteer. So what the crooks would do is say, 'Here's a hundred pounds'. They'll go to wherever, get the hundred pounds or I'll transfer a hundred pounds into your account. 'I need you to go to the Western Union office in Lewisham High Street in London and transfer it to this account in Russia. And, when you do that I will send ten pounds into your account'. So they go and do it. So they passed trust test number one. So the crook, he doesn't really mind, because if the guy runs off with the hundred quid, he's run off with the hundred quid, but when you're dealing in millions does that really matter? So, the next time it'll be five hundred pounds, do it and there's fifty quid in it for you. Next time, it's a thousand pounds, do it and there's a hundred pounds in it for you. And so on and so on until it builds up. And then they get to really trust money mules. 'You know he's had ten thousand pounds from me before and he transferred it and he's really reliable (UK-(F)LE-2).

This connects with some existing support for the idea that repeated interactions among cybercriminals could help build reputations for trustworthy behaviour. For instance, in their study of underground forums, Motoyama et al (2011, p. 75) find that a significant amount of personal messages responding to trading (advertisement) threads came from prior acquaintances. This could mean that, although other factors

[37] Money mules are tasked with moving money rather than drugs, often through non-physical methods like online bank transfers or international money transfers.

might also be involved, cybercriminals on those forums felt more comfortable dealing with existing partners rather than engaging with new ones.

Former North American cybercriminal, Scott, explained how his preference was to work with people he already knew or had worked with previously. Sometimes this meant not dealing with people on forums at all, as he wrote:

> A lot of times you find that a lot of good people wouldn't even be on forums at all (at least not with the same nick or not advertising lol) because they would rather just work with who they knew and avoid the added heat/attention from being on the forums. Once I found someone that could do a certain thing or provide a certain service well or whatever, I would just keep using him until he no longer could, ripped me off, or quit/disappeared or whatever (NA-(F)CC-2).

The second key aspect of cybercriminal reputation online is the important role that referrals and background checks play. While cybercriminals might build a reputation through repeated interactions with other individuals and maintain that reputation through their brand (nick)name, the next question is how information about their reputation may be learned by others not directly known to them. After all, not every interaction between cybercriminals will be part of a long dyadic process, and even those that are dyadic will require the initial step of participants deciding whether the risk is low enough to engage in the original interaction. One possible answer is that information about individual cybercriminals could pass through social networks, via gossip or otherwise, thereby allowing cybercriminals to learn important details about potential partners. But, as Granovetter (1985, p. 490) tells us, a better source "is information from a trusted informant that he has dealt with that individual and found him so".

Referrals play an important role in the cybercrime sphere. As Scott explained:

> If you are not using a forum, then word-of-mouth is another thing people use. If you are looking for someone to provide a service you need and you have some other people you are already working with on other things, its always good to ask them first if they know a good cashout guy, or dumps vendor, id vendor or whatever it may be. Usually, that is your best option (or it was for me) and used forums as a sort of last resort because of the ripper potential and its always better to work with a person that someone you already trust, trusts (ha) (NA-(F)CC-2).

Scott viewed this approach as equally important when trying to avoid partnering with undercover law enforcement (NA-(F)CC-2). It is also possible to list potential referees when introducing oneself to allow others to contact them if they have an interest in working with you. Below is such an example from the forum Ghostmarket:

Figure 2: Referee Post



Source: Ghostmarket

On the Internet, one can also engage in background checks rather than just rely on the word of others. Cybercriminals have the advantage of being able to compare a user's online footprint to the information they have drawn directly out of him (WE-(F)CC-1, NA-(F)CC-2). Such a footprint could include past affiliations with different groups/forums or posts from the individual with relevant information. Of course, as was shown by undercover FBI agent Keith Mularski, who managed to ascend to the top administrator rank of the DarkMarket forum, certain aspects of this trail may be

forged. In Mularski's case, the agent managed to attain the reputation of an elite Polish spammer under the handle Master Splyntr, after being posted on a list of the top ten spammers in the world. The publisher of the list, anti-spam NGO Spamhaus, had collaborated with the FBI on this deceit (Mills 2009).

Some cybercriminals may go further in checking their would-be collaborators' backgrounds. One tool available is to hack into a partner's email or system to find out more details. Scott wrote about how he used to engage in this practice:

> Also, if you are able to conduct a little recon on your partners, it never hurts ;-). I have gotten into partners emails before to make sure I knew what they were up to, also tried to find any link to a real world name etc anywhere else on the internet with that same nickname etc. (some people slip up and use the same nickname they used when playing counterstrike or something for example and leave posts with their real name or something on other places on the internet). The more you know, the better (NA-(F)CC-2).

The final point to note with regard to reputation is that forums have institutionalised this mechanism so it can be applied to sizeable clusters of strangers. In large groups, the cost of requesting referrals or doing background checks on other members would be high. Major forums can have up to thousands of members so it's likely that many users would not know each other or have mutual acquaintances who can make a safe introduction. In fact, as noted in chapter 4, their very presence in the forum, likely indicates a lack of contacts in the first place. As a result, in order to reduce risks, forums and other online institutions have had to find ways of scaling the reputation mechanism to their structures. A number of forums have numerical reputation indices where users can be rated according to their past actions, either by forum officers or all

members depending on the case. These ratings can then be used by members in deciding whether to collaborate with a specific individual (Décary-Hétu and Dupont 2013). Motoyama et al. (2011) find evidence that higher reputation scores correlate to a greater number of private messages from other users (often indicative of interest in doing business). Some forums, like Ghostmarket, also have formal ranks, such as "trusted members" among others, if users prove their "criminal credentials to the administrator and moderators".[38] Such ranks may be a means for forums to provide more tangible evidence of a good reputation.

While these systems might have some value, the empirical data I collected suggests that qualitative reviews and feedback options are much more important in practice. This function allows buyers to provide accounts of their experience of interacting with certain sellers (Holt 2013a, p. 173, 2013b, p. 2). Scott explained the importance of this in choosing potential partners:

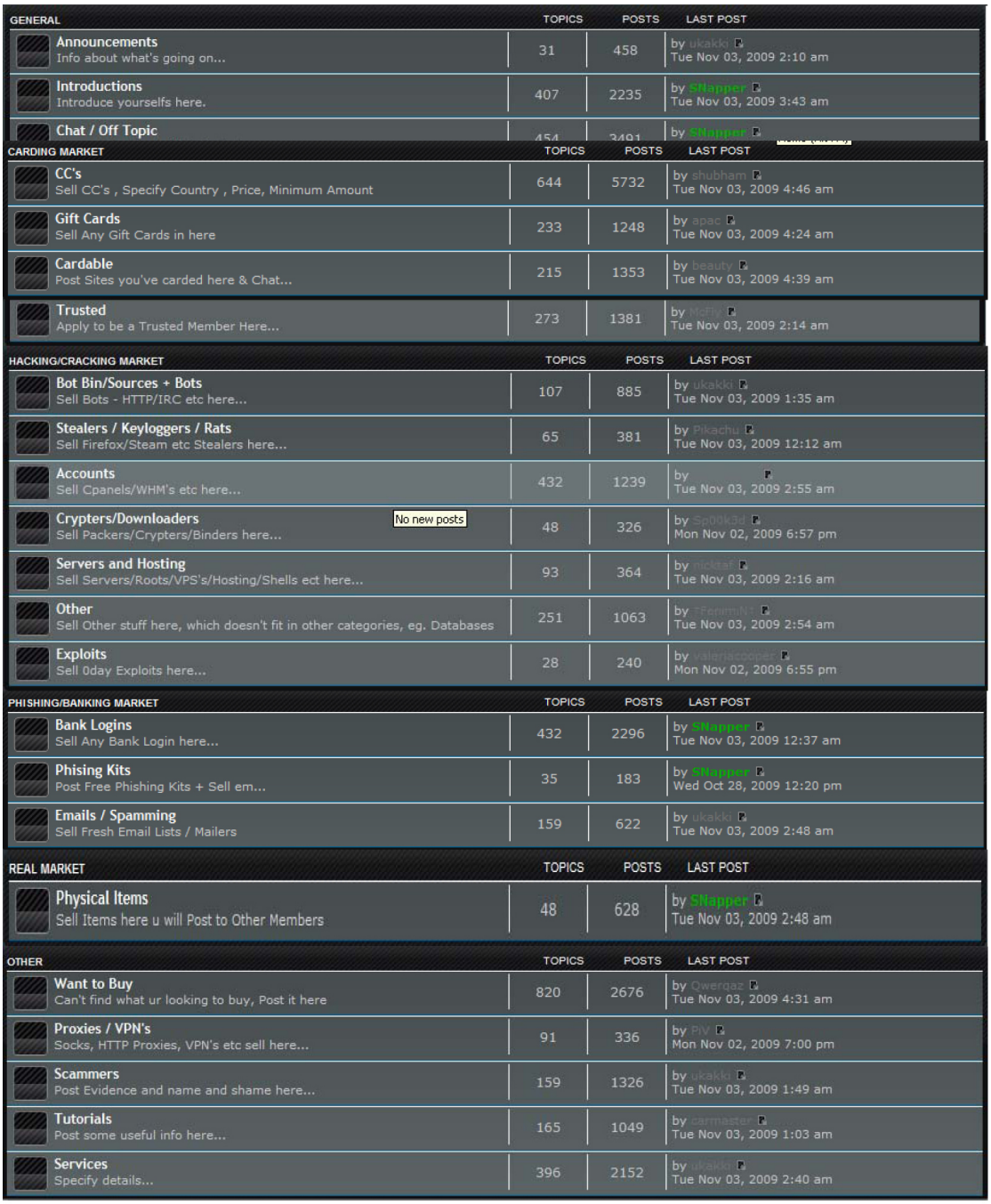
> If you are advertising your service on a forum etc, then you have your own thread where people leave feedback for your service and products etc. Kind of like eBay, you do business with the guy, you leave feedback in his thread saying if he was helpful and legit or not or if you had any problems etc. If you see someone on there that has been dealing with several other people you know for awhile and the people you already know and trust are leaving good feedback, then probably ok to deal with him (NA-(F)CC-2).

The importance of reviews as a reputational measure was confirmed from the law enforcement perspective as well, with a sense they were even more important than various points systems (UKR-(F)LE-2).

[38] *R v Kelly and Others*, Southwark Crown Court, 2011, 35 [Case Summary].

In some ways, an extension of this idea of reviews is found in various “name and shame” sections. These are special sections on forums where cybercriminals can provide evidence of bad behaviour, warning others to steer clear of “rippers” and other malefactors. Being publicly shamed in this way can damage reputations, lead to ostracisation, and can act as a deterrent to other would-be scammers. Below is the menu page for Ghostmarket, which shows the “Scammers” section towards the bottom:

Figure 3: Forum Menu Page with "Scammers" Section



Source: Ghostmarket

The vouching process required to enter some closed forums institutionalises the way cybercriminals regularly seek and provide referrals before engaging with someone. These so-called more elite forums often require new members to be vouched for by at least two existing members (UKR-CSP-1, NIG-(F)LE-1, RUS-CSP-5, RUS-CSP-6). Some forums have even more restrictive tests, requiring upwards of four existing members to provide recommendations, who must have known the prospective member for at least three years. This reduces the need to seek referrals with each new partner on the forum. In some sense, all potential partners are pre-vetted, which signals that the forum is a safe place to do business. To ensure that the recommendations are genuine, there is often a rule that the vouching members are held responsible for any misbehaviour by the new member they have introduced to the community. For instance, they would have to repay anyone who has been scammed or face being banned along with the *ripper* (NA-(F)CC-2).

The above discussion suggests that reputation is very important for cybercriminals to lower the risks of doing business with each other. In order to make sense of how cybercriminals make use of reputation, it is important not to see their approach as entirely novel. This is particularly the case with illicit trading forums, which bear some similarity to legal online auction sites like eBay and employ analogous reputation systems (Dellarocas 2003, Resnick and Zeckhauser 2002, Diekmann, Jann, and Wyder 2009). There are also parallels between reputational systems on forums and offline historical examples from entirely different contexts (Milgrom, North, and Weingast 1990, Greif 1989).

For instance, the Champagne fairs, a major centre of trade in medieval Europe, faced quite similar issues of trust and enforcement and addressed them in familiar ways. In this example, the challenge was that merchants congregated from many different lands and then left, making the subsequent enforcement of contracts difficult. The fairs overcame this challenge with a system of private judges who kept records of merchants' past behaviour, so that before engaging in a deal, traders would enquire with a private judge about their potential partner's reputation (Milgrom, North, and Weingast 1990). Cybercriminal forum reputational mechanisms like reviews, naming and shaming sections and numerical indexes appear to play an analogous role to that of private judges at the Champagne fairs. They effectively lower the cost of users having to investigate personally all other users they might deal with, by providing public information on past transactions within the community. They are a strong embodiment for the importance of institutions in expanding exchange and supporting the development of the broader industry.

Appearance

The data collected for this thesis suggests that appearance is another important way for cybercriminals to demonstrate trustworthiness, but with not quite as much support as for reputation. The way that appearance functions online is somewhat mysterious, even to the cybercriminals themselves. Sean, who worked on the technical end of the spectrum and generally steered clear of those on the money side, explained it like this:

> At the time, we didn't really see age as being a matter. For example, when someone came on we judged them purely based on their ability, their hacking mindset. Your ability to solve problems, your technical how technically minded you are, but

> mostly how quickly you learn. There are a lot of things that give you that hackers mindset. We didn't really judge people based on age, gender anything like that. Females might get a bit more attention. But we didn't judge based on that. A lot of the time, I didn't even know how old any of these people were. I didn't know about what race or anything like that. We just judged people purely on how good their hackers mindset was. And a lot of the time, you just know. It's hard to explain how you know. I can't think of how to explain it. You just get a feeling for how someone is after talking to them on the chat rooms, seeing how they respond, what sort of things they talk about, what sort of things they take an interest in. Very much like talking to someone, like we are talking now. I mean there are no facial expressions or anything like that go into it, but you can still judge someone fairly well just from text I think, sometimes easier… (WE-(F)CC-1).

There is a difficulty in attempting to comprehend appearance in relation to online interactions because many aspects of appearance are, traditionally, physical. Some facets of physical appearance can't be changed or are difficult to do so, such as size, shape and skin colour. Other aspects can be altered such as clothing or hair style, but still remain partially dependent on certain constraints, like budget. On the other hand, online appearance is almost entirely mediated and many aspects can be easily manipulated and faked. Appearance online is much more a construction of a persona. This subsection addresses appearance in these terms. With regard to trustworthiness, it is particularly concerned with potential "tells" that cybercriminals rely on to ascertain aspects of their confreres' "true appearance". In a sense, these are the limitations for persona creation that remain despite the online nature of the interactions. These include: style; language/nationality; memberships/affiliations; and time spent online.[39]

[39] While beyond the scope of this paper, it's possible to view issues of cybercriminal appearance through a signaling theory framework (Lusthaus 2012, Décary-Hétu and Leppänen 2016). On signaling theory more generally see Spence (1973) and Gambetta (2009b).

In terms of style, Scott was in agreement with Sean that cybercriminals could get a sense of a user from the way they wrote and presented themselves. But he was a little more specific about what he looked for. He wrote:

> Usually, you would kind of watch how this person would act in general on forums/chat rooms. Pay attention to how and what he talks about. If he talks allot about un-neccessary stuff out loud and asks allot of stupid questions, or claims to have done things that just don't add up, red flag usually. Most of the people that are serious about business are generally quiet as can be in public (forums/chatrooms) and straight to business over PM's etc (unless you already know them, then you might have occasional chit chat etc) (NA-(F)CC-2).

He also watched for inconsistency in typing patterns or unusual offers/requests. These could be evidence that a nickname had been hijacked, taken over by law enforcement, or that something else untoward was going on (NA-(F)CC-2). On the other hand, style is not entirely beyond faking. Max Butler actively tried to vary his writing style to avoid similarities between his cybercriminal persona and security papers he had written as a white hat or posts made under his real name (Poulsen 2011).

The second key aspect of online appearance is language/nationality, which can play a number of different roles for cybercriminals – some negative, some positive. This factor can deter cybercriminals from dealing with or trusting certain potential collaborators, as is the case with Russian-speaking cybercriminals who are often wary of English speakers. Following successful law enforcement operations against high-level forums in the 2000s, certain Russian-speaking cybercriminals appear to have become more guarded in their operations, choosing to operate only in the Russian language, possibly as a means of keeping out Western law enforcement, or at least

making it one step more difficult for them (see chapter 3). This point was emphasised by a large number of interview subjects (US-LE-2, NLD(E)-CSP-1, NA-(F)CC-2). Nikita, a former Ukrainian law enforcement agent, argued that even if English-speaking researchers and agents could gain access to certain Russian-speaking forums, they would be shunned by most members (UKR-(F)LE-2). Of course, it is unrealistic to think that Western law enforcement agencies and companies don't now employ fluent Russian speakers to infiltrate this space (US-LE-2).

But potential prejudices are not limited to Russian-speakers. While Sean was open to working with a range of people without prejudice, there was one rider to his claim:

> When I said that we didn't bias anyone on race or anything like that. One thing that we did bias them on was their ability to speak English language properly, speak *the* English language properly rather. And usually that meant that if someone was foreign they wouldn't really be accepted into a group because they weren't able to speak English properly. So your groups would usually be separated based on the language barriers. I can't recall of any other previous group where you had intermixing language barriers. Because it is all online, you judge people on how they are typing what they are typing and one of those things if they are not very good at typing in that particular native language, it confuses things a little (WE-(F)CC-1).

In contrast, in some circles, having the right nationality or language can be a positive quality that might even encourage collaboration. Scott wrote that poor English might be a good sign for a "supplier" (of credit card data in his case):

> I seemed to have noticed over the years also that if it is someone that is a supplier of something, if he seems to speak broken English, another good sign since allot of the suppliers come from eastern Europe/Russia (although this obviously can

> be faked but usually not too consistently, you can tell if its real) (NA-(F)CC-2).

Scott provided some detail on the specific tells he might look for in determining nationality:

> Obviously, there is no way to always know if someone is faking where they are from for sure, but you begin to develop a "feel" for it. This falls back on the typing patterns a little. I noticed over time that allot of the eastern Europeans (and non-americans in general) use the word "bro" allot or use words like "university" instead of college, put USD at the end of $ amounts, use the word "market" or "bazaar" when talking about a shopping center, says monies instead of money (makes words plural with "s" that are not supposed to be etc. Also, you can tell if they don't understand U.S. slang words allot (or not well) (NA-(F)CC-2).

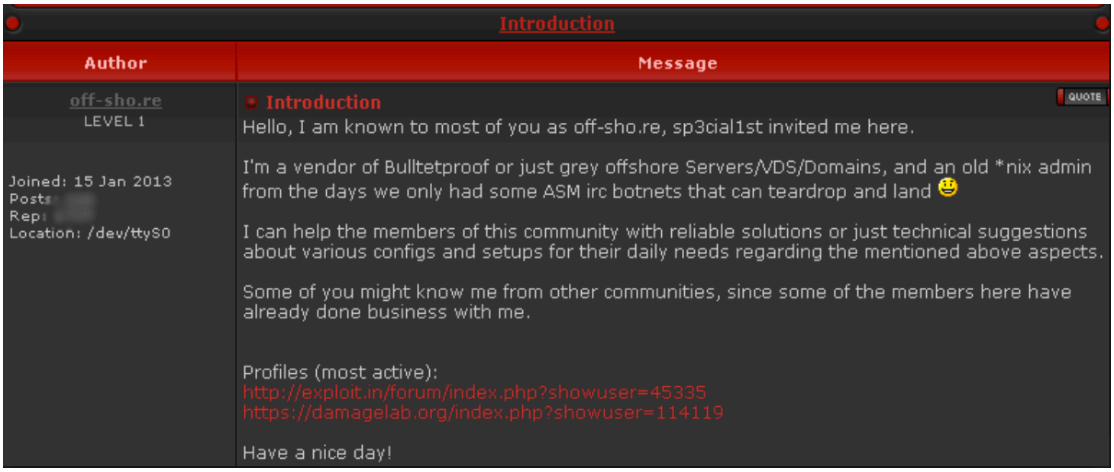
Interestingly, I heard from security researchers who go undercover on forums, that a common tactic is for English speakers to affect broken English in an attempt to impersonate a non-native speaker, which appeared to provide greater criminal credibility (NLD(E)-CSP-1, UKR-(F)LE-2). It's not dissimilar to cybercriminals who pretend to be from Eastern Europe, trying to appropriate their good reputation in the industry (NA-(F)CC-2).

The third significant aspect of appearance is tied to where certain cybercriminals are operating online and what affiliations they have. While this may interrelate with other mechanisms, membership of certain forums and other groups in itself helps create an appearance of trustworthiness. Frequenting the right places at the right times is one approach used by conventional criminals to identify each other, and filter out non-criminals. For instance, when Joseph Pistone infiltrated the Bonanno crime family in

late 1970s New York as an undercover FBI agent, his initial strategy was to frequent "wise guy" bars and establish a criminal appearance by association (Pistone 1987, p. 46). My data suggests a similar phenomenon applies to cybercriminals, but their hangouts are online (UK-(F)LE-2). Parts of the online underground, which are often hidden, are even more difficult to happen upon accidentally. A user who is present in one of these places has to have at least some degree of knowledge and connections to be there in the first place.

This closely relates to the final element of appearance under discussion: time spent online. This is a good indicator that someone is not a "nube", or otherwise a *ripper* or law enforcement agent, in that they have managed to maintain a viable online presence for a considerable amount of time. Some forums, like Darkode, even have a requirement of showing proof of three years worth of online "existence" from other forums, to ensure those new to the scene cannot join (UKR-CSP-1). A number of forums also provide the starting date for each user, which demonstrates how long they have been around for. This can be seen on the left hand side of this post from the forum Darkode:

Figure 4: Joining Date



Source: Darkode

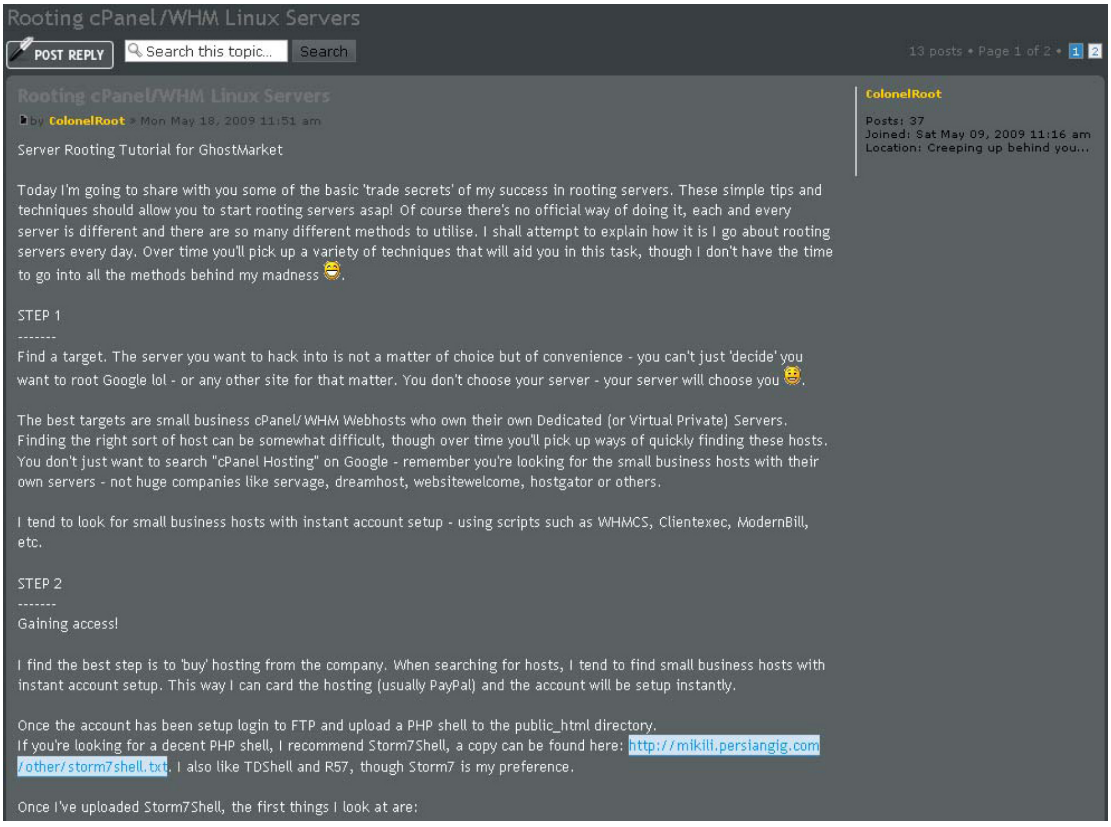
Another more esoteric means of determining whether someone is new to the scene is from their nickname. This was discussed in more detail in the previous chapter. The key idea was that the longer, more complex and "decorated" a nickname is, the more likely that person is a young, immature "nube" (WE-(F)CC-1, NA-(F)CC-2). More experienced actors are often content with simpler, shorter nicknames.

The basic principle here links back to reputation in some ways. The longer one has been around for and attached to a specific nickname or profile, the more time that has been invested. This is a large cost. The bigger investment of time, the less likely someone is to jeopardise it and so the more trustworthy that person becomes. Sean emphasised the large amount of time required to build and, just as importantly, maintain a persona online. Now that he works full-time in the legitimate IT sector, he believed he could never have the time to remain relevant online: it's "really a lifestyle thing" that requires hours and hours of time in order to show dedication (WE-(F)CC-1).

Performance

The data I collected suggests that performance is also an important element in the way that cybercriminals determine trustworthiness, but again with less significance than reputation. This could be either generalised performance or a more specific variety of performance. The more generalised case sees cybercriminals displaying their bona fides as a broad advertisement for their services or goods. For instance, prowess demonstrations can be regularly found in online marketplaces (UK-LE-1). One method of demonstrating a certain skill or piece of knowledge, particularly in relation to less experienced/competent users, is to post tutorials on forums, which often have a dedicated section for this:

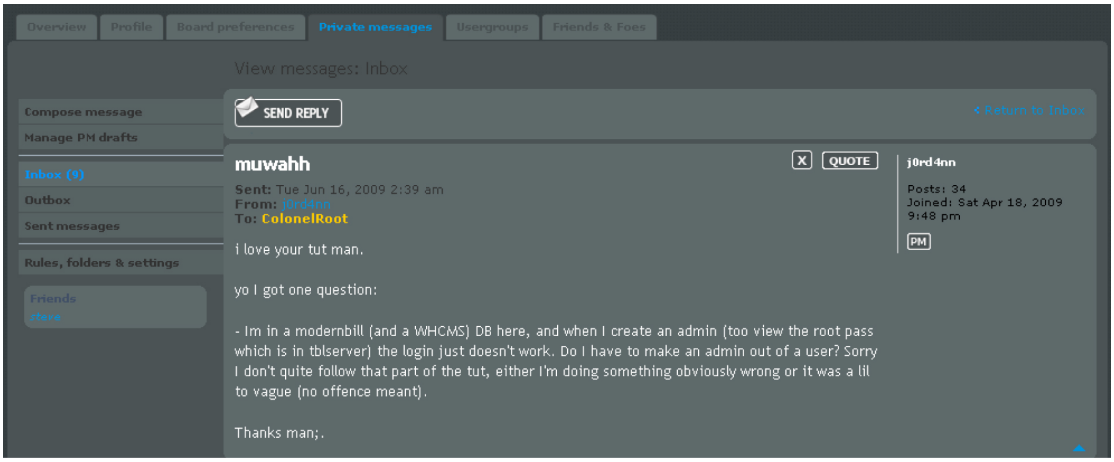
Figure 5: Prowess Demonstration Post



Source: Ghostmarket

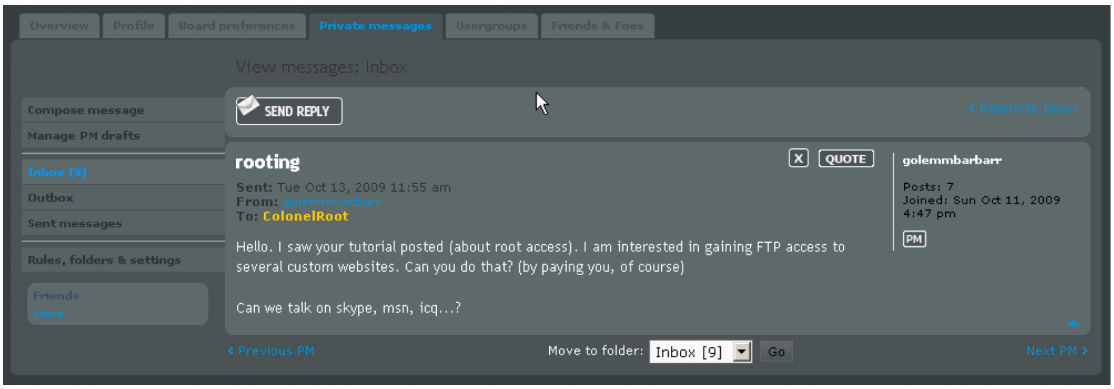
The success of the prowess demonstration can be seen in the private replies that are received in response to it:

Figure 6: Private Message Reply 1



Source: Ghostmarket

Figure 7: Private Message Reply 2



Source: Ghostmarket

Performance also can be less generalised and more specifically tied to a particular criminal endeavour. For instance, the example of money mules discussed above does not only apply to the reputation mechanism. While Phillip's quote demonstrated the importance of repeated interaction in building trust, each step could also be viewed as

a test of performance. By successfully moving on small amounts of money deposited to them, mules may then be entrusted with incrementally larger amounts. For those selling products on forums or in other settings, samples or test buys play a similar role in assuaging any concerns over quality (UKR-(F)LE-2).

In the same way that forums have institutionalised aspects of the reputation mechanism, the performance mechanism has also been incorporated into the structure of online marketplaces. The central way that forums do this is by having forum officers, or those they endorse, test the performance of a product or service on behalf of the community (UKR-(F)LE-2). This reduces the need of individual users to verify the quality of goods in each case, or simply trust that they will be of sufficient quality. In a number of cases those whose products have been verified will receive the title of being a "reviewed" or "verified" vendor, which might also be accompanied by a report on the quality of their goods. Being tested may be voluntary for sellers, but it is not difficult to see how it might help in their sales pitch if they are approved in such a way (Holt 2013a, p. 173, Holt and Lampke 2010, Yip, Webber, and Shadbolt 2013, p. 13). Some also advertise their verified status from other forums they might be on, as a means of attracting more business, as evidenced in figure 3 (see also Holt 2013b, p. 14). In some cases, being reviewed is even a required step before vending:

Figure 8: Verified Vendor Requirement



Source: Lampeduza

Some of the checks employed by cybercriminals don't necessarily relate to the product or service being offered, but are more subtly focussed on assessing prospective, or returning, partners. Scott outlined his approach for assessing new partners, moving beyond appearance to employing clear tests. He wrote:

> As far as online goes, a good place to start when dealing with someone new that doesn't have much of a reputation is my talking to him and trying to see if he, in general, knows allot about the scene and terminology used in it as well. You can proceed this by asking questions that only someone that is actually a real worker would be likely to know off hand. For example, you could start up a conversation about common problems you have with certain brand ATM's, printers, software etc and see if the guy can elaborate on it, or you could go the opposite way and make something up about it and see if he tries to agree with you on it (which is an obvious red flag). If he were to correct you, you could be like "oh yea, I was thinking of something else" or whatever. If, overall, he seems to be familiar with what he claims to do off hand (not over email, I'm talking about in real time chat, ICQ/IRC/Jabber whatever) then its a good sign (of course not for sure though) (NA-(F)CC-2).

Scott explained that it was important to carry out this evaluation in real time chat so that there was no opportunity to fabricate answers. If the person cannot provide immediate and credible answers then the level of suspicion would increase. But it is not certain that someone who can't provide answers is a *ripper*. It may also be the case that the person is a "reseller" who must check details with the original seller. Being a reseller is not a problem in itself, but it was Scott's preference to deal with original sellers where possible (NA-(F)CC-2).

Scott thought similar tests were appropriate when trying to determine whether a formerly reputable nickname had been compromised or was being impersonated,

either by law enforcement or a *ripper*:

> If someone drops off out of nowhere and you haven't heard from them in a long time and they come back talking kind of strange with some weird excuse, its always good to ask a verification question from the past that only they would know, just to make sure you are talking to the same person (although you can usually tell because of their typing patterns etc after awhile). Gotta try to make sure you are not talking to LE directly (although they could be working with them) or someone that hijacked their account, trying to rip you off (NA-(F)CC-2).

A suitable "verification question" might refer to a shared password from old business together, knowledge of who first introduced them to each other, or what project they first worked on together (NA-(F)CC-2). The ability to answer such questions in good time, would also be important. This links to the appropriation of nicknames that was discussed in the previous chapter.

This discussion leads to a more general point of how cybercriminals can determine if other users are undercover agents. Performance appears to play a key role here, specifically relating to proof of one's criminality. Don, formerly an elite cybercriminal believed there was only one true method that could unmask agents:

> The only consistent manner of uncovering American law enforcement is to get them to do something that they and their turned individuals cannot do. Usually in the USA this means getting them to hack a site, or abuse some piece of information that you know is an innocent third-party. I have often seen undercovers pretend to provide dumps in or other resources but those were actually bogus accounts set up as part of an agreement with the bank, so the account was really not owned by a person, and therefor didn't break laws – they were giving away their own credit cards, basically (NA-(F)CC-4).

This dovetails into the idea of *display crimes*, which are designed to provide proof of criminality. In conventional crime, the most stringent of such tests often involve carrying out a murder (Gambetta 2009a, pp. 16-18). In cybercrime, the stakes are lower, but this performance test operates in a similar way.

Enforcement

Aside from elements of trustworthiness, enforcement is the other mechanism that enhances cooperation among cybercriminals and has allowed the formation of an industry. This mechanism can function even when there is little trust between parties. Enforcement can be carried out in three main ways: self-enforcement; collective enforcement by a group; or enforcement by a third party who may act on behalf of an individual or group. As noted in the introduction, monitoring and sanctions offer the simplest forms of enforcement. Establishing a credible commitment can also buttress cooperation. This can be done through third party enforcement, or through a more esoteric means like cutting off options or exchanging information hostages.

Cybercriminals only have limited enforcement options available when operating independently of online structures like forums. Unlike in an offline context, they cannot employ violence. In very basic terms, cybercriminals can sanction recalcitrant partners by refusing to continue cooperating with them. But cybercriminals also have some more punitive options open to them, including tools that appear to parallel the use of violence, but in weaker virtual terms. For instance, in the hacking group that Dupont (2014) studied, an alternative method of enforcement is described: the use of

botnets to attack other hackers online. It can be used collectively by the group against certain recalcitrant members or by members themselves against other members as a coercion or punishment tactic. Similar attacks have been used by competing forums against each other (Poulsen 2011, p. 168). Their use is a relatively common cybercriminal tactic online (NA-(F)CC-2, NA-(F)CC-2).

There are also other forms of cybercriminal punishment that have developed. "Doxing" involves the digging up of personal information and then publishing that information online to embarrass the person in question. It also effectively removes their anonymity, which is the most treasured possession of any self-respecting cybercriminal. Scott provided an example from his time online in relation to the downfall of a key cybercriminal player, writing:

> …there are also sometimes reprecussions for "ripping" etc. Take, for example, one cashout guy I used to know whose nick was XXXX[40]. His downfall came from under-estimating his supplier and deciding not to pay him $40k. Not soon after the rip was confirmed, he was kicked out of the IRC channel (where he was an operator at the time), banned from it, and the topic was changed to "Whoever wants to fuck XXXX click here". The link was to a page (on a hacked banking site lol) that had his picture, name, brothers name, address, phone, swift account #'s, bank acct numbers etc. Two to three weeks later he was busted (NA-(F)CC-2).

This example demonstrates the seriousness of this form of punishment. Not only does it lead to embarrassment and a sense of violation, it also allows other actors online to make use of the posted information and engage in further violations, whether abusive or involving theft or fraud against him. More importantly, it may aid law enforcement

[40] Name removed to maintain anonymity.

in apprehending that person. *Doxing* can be carried out by any aggrieved member of the online community, but there are also professional *doxing* services that exist. These are people with a particular talent for this activity and offer their services for hire (NA-(F)CC-2). DDoS services can also be hired, but they often have more "legitimate" purposes than targeting other cybercriminals, such as extorting businesses whose trade relies on online sales.

"Swatting" is another punishment activity related to *doxing*, which is sometimes carried out by the same people. This involves duping emergency services into sending armed units to someone's house or otherwise, under the mistaken belief that there is an ongoing incident. One famous example of *swatting* involved leading security blogger Brian Krebs, whose reporting is based on deep access to cybercriminal forums. It is not uncommon for Krebs to aggravate a number of cybercriminals with his work, sometimes leading to threats. In this case, the blogger was surprised to find heavily armed police outside his home one evening, who immediately apprehended him. The event became the subject of a widely read and publicised post entitled: "The World Has No Room For Cowards" (Krebs 2013).

These forms of punishment indicate how information can be used to cause damage. Gathering information also plays an important role for the purpose of monitoring, perhaps with later punishment and coercion in mind. Scott outlined how seriously he took this task, writing:

> I used to make a little notepad on each person I was suspicious of (or trusting allot of stuff with) and keep track of any little clues that I could get. Allot of times, people slip up and say or do things they don't mean to or don't think about. You have to

> pay attention to the details. Anything you can get that you can use to try to find more out with, save it in a file to create a profile on them kinda. Any email addresses they use, nicks that they use, ip addresses and even meta-data from pictures they send could be helpful. Anytime they send money with WU or MG etc, keep any names that they use. There are allot of people that will actually use real names (or close variations of) to do this or names of other people they know. You keep any addresses that you might have got from them (from mailing physical items). You could also do teamwork kinda with anyone else that might be involved. For example, if they were buying ID's or plastics from someone else you know well and work with, ask them if they have the addresses or pictures even that were used in their order. If you already know the seller better than them and let him know they ripped you, they might give it up (or sell it to you lol). You could always go with the virus approach if you thought you could pull it off and were really suspicious, but you better be pretty sure with what you are doing if you don't want to loose them (because if they figure it out they will not take it well). If you have a custom version of a key logger that is crypted just for that use that wont be detected most likely then try it out. Also, one thing that helps is addresses on receipts that are sent as pictures for verification possibly and if they happen to have a hand or something in the picture you could possibly tell their skin color (NA-(F)CC-2).

Even in cases where there isn't any suspicion, the gradual exchange of personal information often takes place over time between long term partners, slowly chipping away at their anonymity. Former cybercriminals interviewed for this project provided examples of speaking on the phone to certain collaborators and sharing personal details about their families, offline lives and so on (WE-(F)CC-1, NA-(F)CC-2). Such behaviour was not widespread and usually reserved for certain partners, who had already established a degree of trustworthiness. But it goes against the idea that anonymity should always be maintained by cybercriminals as a core norm. Even more curious are the cases of cybercriminals meeting each other in person that will be discussed in chapter 7.

One possible explanation for this behavior can be tied to Schelling's idea of information hostages. To restate the central idea from the introduction: rather then handing over people, an information hostage involves the exchange of compromising information. The process encourages cooperation because each side has the power to incriminate the other. This serves as a credible commitment. In line with this theory, once cybercriminals feel comfortable with each other, they engage in an exchange of personal information to cement the relationship. In the context of forums, some similar processes have been observed. DarkMarket, required those who wished to join to submit the details of 100 compromised credit cards. These would be verified by two reviewers, who would provide reports on their legitimacy. As one investigator in the case explained, if "the cards did what they were supposed to… they would be recommended. If not they weren't allowed in" (Davies 2010). This mirrors similar attempts in the non-profit sphere, such as online paedophile groups that require the provision of a certain number of original child pornography images in order to join (O'Neill 2001).

But in subsequent years, similar practices do not appear to be widespread among forums. Such examples appear to be relatively rare, at least in the profit-driven sphere. While verified vendor status commonly requires goods to be vetted by forum designates, they have not been popular tests for basic entry into forums. In recent years, closed forums seemed to have valued other tests like existing members vouching for new members. This is perhaps an admission that tests like the DarkMarket example can be defeated by law enforcement with the assistance of banks (but it might still keep security companies or *nubes* at bay). Instead, the primary

application of information hostages appears to be with regard to offline relationships, which will be discussed in chapter 7.

Aside from information hostages, forums formalise and expand aspects of private enforcement to keep cybercriminals in line. This brings the enforcement mechanism to an institutional level and scales its impact to much larger numbers. The most widely documented sanction is exclusion from a forum by order of the administrators or moderators (Holt 2013b, Holt and Lampke 2010). Administrators make the rules of forums and they can enforce them by the means they deem necessary (Holt 2013b, p. 11). My data confirms that banning is a common form of punishment and a relatively powerful tool (UKR-CSP-1). But there are complexities involved. Scott wrote that sometimes bans might not be indicative of bad conduct, but rather biases of certain forum officers, who might be abusing their power or "hating". As a result, those considering dealing with someone banned from a certain forum would best investigate further: "If it seemed like it was minor bullshit and possibly biased by the administrator or whoever, then you could still proceed if you thought it was worth it but obviously, be careful and take it as a warning ;-)" (NA-(F)CC-2). On the other hand, if someone had been banned from a number of forums, then they are best steered clear of. In a sense, the idea of banning again links back to the reputation mechanism:

> Your best bet is to check into the feedback to see if other people (that you already trust/deal with) left feedback and talk to them and get their opinion. Overall, if it seems like the nick is banned for good reasons on a respectable forum, then that nick is basically dead. They could start over with another nick if they wanted to and build back up, but it would take time and more positive feedbacks to get it back up. Sometimes people can figure out if its the same person though just by typing

> patterns or whatever and everyone will be scared off (NA-(F)CC-2).

The key weakness with regard to banning as a means of punishment is that offenders can attempt to rejoin that forum or others under a different nickname. The users themselves are not banned, only their brand names. Cybercriminals often rejoin forums they have been excluded from with the true cost of the banning being the need to rebuild a new reputation from scratch. Though important, such a cost is far less than the sanction of being purged from, for example, a mafia group – conventionally death.

Linked to banning is the arbitration role that forum administrators often perform. The process is akin to an online trial. Nikita, the former Ukrainian agent, provided an outline of how this might work in the Russian speaking underground. While the arbitrator can be a forum administrator, in the Russian scene it is common for something nearing professional specialist arbitrators to exist, including one known individual who was commonly called in to judge disputes across a number of different forums (UKR-(F)LE-2). Nikita described the arbiter's job:

> It's his role to research all the evidence. The guys present evidence and the usual evidence is the chats. So they usually communicate through Jabber and mostly they post chat logs or screen shots. In some cases, if it involved malware for example, they might give access to that malware control panel, for example, to the arbiter for him to see to test it and then after these several posts by both sides providing their evidence, the arbiter makes his decision. The usual decision is to expel the party that was involved in wrongdoing (UKR-(F)LE-2).

It is also not uncommon for others to have a say on the matter: “It’s kind of like regular court hearings, but online in the underground world. There are witnesses, evidence, the judge – the arbiter – who makes the decisions” (UKR-(F)LE-2). A similar process takes place on the English language forums, but the arbitrators are often forum administrators rather than professionals hired to perform the service (NA-(F)CC-2).

Forums also make use of another tool to enforce agreements directly: escrow. Escrow services are provided by forum officers in some cases, but other forum members can also offer this service, if they are able to garner sufficient trust (UKR-(F)LE-2, UKR-CSP-1, NA-(F)CC-2). The third party guarantor holds the money until the goods have been received/verified, but it is also possible to be the point of transition for both vendor’s goods and customer’s money. Guarantors can require payment, often in the form of a percentage of around 3-5% (UKR-CSP-1), but do not always (Yip, Webber, and Shadbolt 2013, p. 14, Holt 2013a, p. 173, 2013b, p. 11). DarkMarket provided a good example of a forum providing escrow services (Davies 2010).

The presence of escrow in the cybercriminal underground is regularly noted, but how it functions in practice is rarely discussed in much depth. Scott provided further details of when someone might use escrow, writing:

> Also, there are escrow services that are usually offered by some of the higher people in the forums (Admin, Mod's etc). If you are doing a big deal with someone (say you are purchasing an entire database of dumps for $30,000 for example) and you want to make sure this person doesn't just take your $30k and run off, you would contact one of the escrow providers and ask for help. This way you have a third party (admin) that takes the $30k in bitcoins or whatever and holds it until you confirm to

> him that you received the dumps you purchased and then he will take his fee out (5% or whatever he charges) and sends the money to the seller (NA-(F)CC-2).

But questions also remain regarding how the escrow providers themselves are deemed to be trustworthy. This point again returns to reputation. Those who perform the role of escrow providers must have an excellent reputation. They are usually "wise old men" who have been around the scene for a long period and have invested considerable time in building a reputation for honest dealing (RUS-CSP-5, RUS-CSP-6). They might be administrators or high level moderators, who are known to be trustworthy. But it would not be sufficient to be the administrator of a small new forum, with little reputation of its own (UKR-CSP-1, NA-(F)CC-2). While 100 per cent honesty is impossible, it is very rare for a guarantor to engage in a scam, as to attain such a role requires a reputation earned over a number of years. Maksym, a Ukrainian security researcher with government experience, described the idea of a guarantor cheating as extremely rare and being like a "nuclear explosion" (UKR-CSP-1). Such a person has the "ultimate reputation" and preserving that hard earned reputation is actually a large part of how those individuals can make money (NA-(F)CC-2).

It is clear that forums enlarge the role that enforcement can play for cybercriminals. Outside of forums, one must rely on self-enforcement or the help of other friendly individuals. But this approach makes dealing with anonymous strangers, who are not closely tied to one's existing contacts, challenging. It limits the extent of exchange that can take place. In line with Douglass North's views, it appears that forums and related groupings have developed institutions to enhance enforcement (North 1991).

They create some order in a chaotic world. But the degree of private enforcement provided by these sites suggests an even further step. In cases where the forum hierarchies establish a system of rules and punishments, guarantee transactions and arbitrate disputes, they are essentially providing a form of governance. As such, they begin to act like some traditional organised crime groups that seek to control the offline underworld. For instance, the Italian American mafia guaranteed trade of bootlegged alcohol during Prohibition. They protected the supply of alcohol, the makeshift "curb exchanges" that served as marketplaces, and the transactions that were carried out at these exchanges (Varese 2011, pp. 114-120).

Ultimately, forums likely fall just short of being accurately classified as mafias or other organised crime groups. Forums appear to comply, at least partially, with the theory of protection, where mafias operate in low trust environments and provide protection for otherwise unstable transactions (Varese 2001, Nozick 1974, pp. 3-25, Gambetta 1993, ch 1). As such, they move towards the definition of a mafia as an organised crime group that "attempts to control the supply of protection" (Varese 2010, p. 17). But while such forums perform mafia-like functions, it is unlikely they could classify as mafias themselves. There are two main reasons for this. First, attempting to *control* the supply of protection is very challenging online. While there is some competition/friction between forums, there isn't a rigid sense of territoriality in the world of cyber. Low barriers of entry mean that other protectors can easily emerge from across the globe. Forums also provide a relatively weak form of governance because enforcement is not physical, but virtual. While the modes of enforcement online appear to significantly enhance cooperation and exchange, they are still a shadow of the most powerful offline sanction: death. Exclusion is an online

version of death, but it is really only a form of severe reputational damage. As was noted in the previous chapter, old nicknames can be discarded and a new identity built. But death is final (see Lusthaus 2013b, pp. 4-5).

The second challenge in conceptualising cybercriminal forums as a form of mafia, is that these structures are not true criminal organisations at all. Don, who played a key role in running a large forum, described the view that forums are one large organisation where everyone works for a boss as "batshit insane". Instead he thought it was more like "running a coffee shop with a bunch of whiteboards where visitors could scrawl notes" (NA-(F)CC-4). In essence, forums are marketplaces, somewhat ephemeral and the individuals behind them - the key forum officers – appear to lack the tight structure and cohesion that might define a bona fide criminal organisation such as offline mafias. In basic terms:

> A mafia is not a marketplace. A mafia may attempt to govern various marketplaces, but its existence is distinct from the individual enterprises it is involved with. For instance, while the mafia oversaw the curb exchanges during Prohibition, this was not its sole occupation as it was involved in a number of other activities. Likewise, while the Sicilian mafia has controlled the Palermo fish market for some time, the fish market is not itself a mafia. The Sicilian mafia is the mafia (Lusthaus 2013b, p. 5).

Governance in the cybercriminal world is largely tied to specific sites, rather than autonomous criminal organisations. Their policing role looks more like the private judges of the Champagne fairs who regulated trading specifically in those marketplaces (Milgrom, North, and Weingast 1990). If merchants didn't abide by their rulings following disputes, these judges could exclude the recalcitrants from entry to future fairs. This is very similar to the way forum officers exclude *rippers*

from their marketplaces, which also acts as a deterrent to would-be scammers and provides a general guarantee that the sites are a safe place to do business. In both contexts, it is clear that institutions are enhancing opportunities for exchange and leading to economic development. Both cases clearly demonstrate some level of governance, but are lower down the extra-legal governance scale when compared to genuine organised crime groups that attempt to govern not only specific marketplaces but entire illicit markets. Nonetheless, regardless of these limitations, the role of institutions and governance in cybercrime has been fundamental, effectively transforming small-scale trade into a bona fide industry.

Risk for Reward?

The mechanisms discussed above are built around the central idea of reducing risks in transactions that thereby increases cooperation. But these mechanisms will never be completely successful in wiping out defection. As noted in the introduction, universal cooperation is far from possible, even in mature societies with well functioning institutions and strong governance. To trust is to accept a certain level of risk. But the other part of the equation is the possible rewards for that trust. If they are high, some might be willing to take the risk. As such, cybercriminals may engage in their enterprises not just because of lower risks, but also because the rewards become so great that they might outweigh the risks in question. Drawing on the interview data, this certainly seems plausible.

Some might question why cybercriminals operate online at all. The simple reason for this is that they can still make money, even accounting for the downsides of the

anonymous industry. While figures can vary and are not beyond critique, it should not be forgotten that the cost of cybercrime is regularly estimated in the hundreds of billions (Center for Strategic and International Studies 2014). Many cybercriminals appear happy to accept the costs of doing business in return for large benefits they can reap. Scott believed that the "bottom line is you are always taking a bit of a risk or gamble, but when you do finally get a good team together, you keep it as long as you can" (NA-(F)CC-2). Lance was a little more forthright: "you got ripped off…? Guess what, you're in the business of stealing money, you're going to get ripped off. Suck it up and carry on with your business" (NA-(F)CC-3).

A similar driver appears to apply in relation to the threat of law enforcement. While those who are arrested might now see the folly in this view, a number of cybercriminals feel that their anonymity protects them against arrest (NA-(F)CC-2, NA-(F)CC-4). To ensure this protection, they have to take the appropriate steps of maintaining good security and not engaging in activities that might give their identities away, such as using non-anonymised payment systems or mailing physical items (NA-(F)CC-2). But once these precautions are taken, dealing with undercover agents is part of the business. As long as there are profits to be made, collaboration may still be worthwhile. As Don wrote:

> In most cases of "trust" relations in the underground the underlying truth is that trust as we are used to thinking of it does not matter, what is important are the deliverables and the results. In other words, if a spammer buys access to an RDP to mass mail, and the server is really owned and operated by FBI, that doesn't really matter to him or her so long as emails are actually delivered and there is a profit, Likewise, when I waas selling credit card data (ugh), then it didn't matter if my customer was LE because their money was as good as anyone elses. It didn't bother me at all and in fact I would greatly

> prefer to have sold all of my stock en-masse to a single LE, becuase that was everyone would be happy – I'd get the money, the owners of the cards and the banks would not "lose" (really it would be insurance and FDIC), and the LE would get their score. But, sadly, for some reason American LE don't buy cards to get them off the underground market, which is an awful waste (NA-(F)CC-4).

Former cybercriminal Jim wrote a very simple and direct answer to the question of why cybercriminals engage in the business when facing risks of scams or arrest: "$, Greed" (NA-(F)CC-5).

The data referenced above perhaps leans towards a picture of the online underground as a trustless world where large profit margins are the primary driver of cybercriminal collaboration. Cybercriminals appear to essentially ignore, or choose to overlook, the risks in the face of what can be gained. There is also an element of pure risk taking behaviour at certain points. Lance summed this up with his view that sometimes cybercriminals throw caution to the wind and just say "fuck it, let's do it" (NA-(F)CC-3). These are certainly important factors to make clear. The rewards of cybercrime play a significant role in driving cooperation. But it's also important not to overstate their importance. This element of reward does not demolish the central significance of trustworthiness and enforcement, enhanced by institutions and governance, or even replace them as the primary factor in explaining cybercriminal cooperation.

As the earlier sections in this chapter attest, there is very strong support in the data for the role that trustworthiness and enforcement play in enhancing cybercriminal cooperation. For instance, all former cybercriminals in this study bar one indicated

that reputation played a key role in deciding who to work with. This is true for Lance and Scott who are cited just above in support of the importance of large rewards in cybercriminal decision-making. It is also true for Jim who noted that greed was of vital importance, but also that "I guess what most people do is try to find a few people they can work with and just stick with them" (NA-(F)CC-5). It was only Don, quoted at length above, that viewed profits as the defining factor in cybercriminal cooperation and didn't really convey the idea of having much trust with partners at all (NA-(F)CC-4).

For the others, there appeared to be clear caution about potential partners, but a sense that they certainly trusted some people more than others and had certain people that they would not do business with. A number also clearly differentiated between different forums and how safe they were to do business on (NA-(F)CC-2, NA-(F)CC-3). Sometimes they might act a little recklessly, but there was usually some calculation involved. It seemed to be a badge of honour when certain cybercriminals believed that they successfully avoided engaging with someone who later turned out to be an undercover agent or serial scammer (EE-(F)CC-2). There is of course tremendous distrust in the cybercriminal underground. But it doesn't mean that cybercriminals all retreat into a nihilistic view of collaborators and simply give up on trying to assess which partners are worth doing business with and which partners should be avoided.

In short, there appears to be little evidence that cybercriminals simply engage with partners indiscriminately. The rewards of cybercrime are why this criminal industry exists in the first place. Without the payoff there would be no cybercriminals, so it is a

vital point to note. But, within this world of suspicion, trustworthiness, enforcement, institutions and governance still play a key role in driving cooperation. In most cases, cybercriminals make use of these elements to reduce the risks involved. They may also be tempted by the significant rewards to encourage deal-making in certain cases, but this supplements rather than replaces the above mechanisms.

Failures of Cooperation

This section addresses a key aspect of social science methodology. If one wishes to study the presence of a phenomenon and the factors that lead to it, one also needs to examine cases where that phenomenon is not present. Some aspects of variation must be included within the sample. In other words, it is important not to select on the dependent variable (King, Keohane, and Verba 1994, pp. 129-137). As this chapter examines how cybercriminal cooperation is achieved so that an industry could be established and maintained, it is also vital to address cases where cooperation among cybercriminals is less than successful.

The most effective way that variation can be brought into this study is through examining historical shifts in cybercrime and the levels of cooperation at each point. As outlined in chapter 3, the early days of profit-driven cybercrime, before the turn of the millennium, were large characterized by lone wolves and limited collaboration. This all changed with the birth of forums and effectively the buttressing of mechanisms that enhance cooperation. As Lance pointed out, one of the fundamental problems of the era of IRC platforms was that no "record" of conversations was available so that one could not get the "vibe for the seller or the buyer to see if they

were able to do business, if they were able to trust them" (NA-(F)CC-3). This was a fundamental problem of identity and branding.

Forums overcame this challenge and made it easier for cybercriminals to review past posts and essentially assess the reputation of other users. This then also allowed some aspects of enforcement to be applied to these identities. The institutional and governance aspects of forums also assisted with increasing cooperation in these communities, by formalising the reputation, performance and appearance mechanisms, as well as extending some aspects of enforcement like punishment, arbitration and guaranteeing certain transactions. As a result, trade began to thrive and the underground rapidly expanded in both size and reach. Firms of various sizes began to form. A strong case can be made therefore that these mechanisms lowered the risks and thereby genuinely improved cooperation between cybercriminals. In the pre forum world, in the absence of these mechanisms, the risks were higher and cooperation was limited.

This approach can also be taken one step further by including the state of affairs after this Golden Age of forums. As recounted in chapter 3, after it emerged that ShadowCrew was run by a U.S. Secret Service informant and undercover FBI agent Keith Mularski ascended to the rank of administrator on DarkMarket, further distrust was injected into the underground. Following these law enforcement successes, cybercriminals became much more wary of who they dealt with. While large forums still exist, a number of experienced players retracted into smaller groupings of more trusted partners. They only engaged with the forums and strangers when they had to out of necessity, such as in Scott's case when his old partners disappeared (NA-

(F)CC-2). The direct suggestion is cooperation levels dropped as the risk increased: law enforcement agents might be lurking online and are capable of carrying out arrests against online criminals.

But further than that, law enforcement appeared to damage faith in cybercriminal institutions. Forums, those places that successfully expanded the operation of key mechanisms to allow successful exchange among large groups, were no longer considered safe. Cybercriminals came to close ranks and rely on trustworthiness even more, and especially reputation, with a strong preference to work only with long-term partners of good standing. Some degree of enforcement is also still possible, but it is less than forums provide. By regressing into smaller groups, wide-scale cooperation is stunted, but small-scale collaboration can still succeed. This is a clear illustration of the value of trustworthiness and enforcement, along with institutions and governance in particular.

Conclusion

In order to build a successful industry, cybercriminals must be able to operate an online environment, despite the risk of dealing with anonymous partners who are criminals. This world is filled with opportunities for defection. The present chapter examined how cybercriminals have overcome this challenge, leading to successful collaborations on a wide scale. It addressed the value of trustworthiness, along with the importance of virtual enforcement. In addition, it also outlined how high rewards might also be a factor in encouraging cooperation when risks abound. Finally, as a

point of comparison, it considered instances where cooperation has been relatively unsuccessful.

Some key points emerged from this discussion. First, in an online setting, reputation is the mechanism of central importance. It was mentioned by numerous participants as the key factor in deciding whether to partner with a specific cybercriminal. While appearance and performance played some role, time and again the data suggested that reputation was of the greatest significance. Reputation also compared strongly to enforcement. This is perhaps not surprising, given that virtual enforcement is relatively weak. But in an online environment, it's also possible that enforcement becomes a manifestation of the broader reputation mechanism. The punishment of exclusion from a forum or other grouping, is ostensibly the loss of a nickname's reputation leading to the associated costs of having to build a new brand. Third party enforcement by means of arbitration or escrow is ostensibly transferring the risk associated with transactions to a more trustworthy third party, who has invested significant time and effort in building a spotless reputation. The risk is lowered by relying on these reputable middlemen, and as a result cooperation is enhanced.

The second key point is the importance of institutions and governance in expanding the industry. This argument has been made above, so I will not labour it. In short, forums appear to be important providers of cybercriminal governance. The institutional order they deliver greatly enhances cooperation and scales it from intimate groups to an industrial level. Forums suggest a possible hybrid of self-governance and private governance. In terms of self-governance, the main contribution of these online marketplaces is to extend the reputation mechanism so

that information can be transmitted beyond a small group of cybercriminals. Instead of past interactions alone, or referrals, providing information about specific users, in forums a tradition of trust could be envisaged as much between pairs of co-operators as it is between each user and the whole community, making compliance, rather than cheating, more attractive (Dixit 2004, p. 12). But while users can collectively choose not to cooperate with a scammer once he has been outed, in practice the enforcement aspects of forums look more like private governance. Forum officers create rules and directly police scamming and other misbehavior. They can provide guarantees for certain transactions and arbitrate disputes. But though significant, this private governance never quite reaches the levels provided by offline mafia groups who seek to govern a number of different markets.

These elements have allowed the flourishing of the cybercrime industry online. Yet no matter how sophisticated cybercriminal institutions may become, some risk will remain. As noted previously, this is the case in all human contexts. But in cybercrime, while the risks have been reduced to a manageable level, the overall problem of distrust remains more intractable. Part of the reason for this is the same as why reputation is so important in an online environment. It's because virtual enforcement remains so weak. Even the most aggressive forms of online enforcement, like *doxing* or banning, pale in comparison to the ultimate offline sanctions of physical harm and death. The shield of anonymity on the Internet makes monitoring and enforcement far more difficult. These continued challenges may help explain the subject of the next chapter: the offline dimension.

7. The Offline Dimension

The role that offline interactions play in a number of cybercriminal enterprises is often overlooked. The stereotype of cybercriminals is of those who operate in the anonymous spaces of the Internet, wreaking havoc that cannot be tracked. The offline dimension is also not widely discussed in the literature. This creates the sense that cybercrime is almost exclusively an online phenomenon, when in reality it is always anchored in an offline context somewhere in the world. In all cases, behind every attack there are one or more cybercriminals who exist somewhere physically. In certain cases, these actors are known to each other in person, or come to know each other over the course of their dealings. This offline element was apparent in chapter 3 across a number a range of instances. Perhaps the best-known example that was discussed was the CarderPlanet conferences, which brought cybercriminals from across the world together to discuss their affairs. This was essentially an extension of the online aspects of the forum. But in other cases, offline interactions appear to be the starting point of cybercriminal cooperation, which may hardly go online at all.

This chapter seeks to highlight the importance of the offline dimension to cybercrime. This dimension is somewhat counterintuitive and perhaps puzzling at first. But with some thought, it is a logical extension from the conclusion of the last chapter. Through the mechanisms that were discussed, online cooperation among cybercriminals has been surprisingly successful. But some risk has remained. Actors remain cautious about dealing with anonymous strangers. The size of firms is relatively small, often limited to just a handful of people because trust will extend no

further. The focus of this chapter is on how offline dealings further overcome the challenges to cybercriminal cooperation and have allowed the greater expansion of the industry. Cybercriminals can feel more comfortable dealing with partners that they physically know. Firms can operate on a much larger scale, with more employees, fixed office space and company hierarchies that include multiple divisions. One can become so focussed on the benefits of anonymity in protecting cybercriminals from investigation, that one can forget that anonymity also brings great costs in terms of distrust. It may actually be an unwanted burden for many cybercriminals.

In short, this chapter argues that, for some actors, the puzzle of cybercriminal cooperation is solved with a very basic solution: choosing to collaborate offline instead of online. This offline collaboration then supports a larger and better functioning cybercrime industry than is possible through online interactions alone. In this case, much more sophisticated organisational structures can develop. This chapter proceeds in four sections. The first section of this chapter outlines the presence and significance of the offline dimension in cybercrime. The second section examines why this form of collaboration is occurring. The third section investigates failures of cooperation in an offline setting and what this teaches us about the topic. The final section addresses the reality that it's unlikely that all cybercriminals will seek to operate exclusively offline or online. Instead they will choose the risk profile that best suits them, their context and their activities.

Offline Interactions

Much of the focus on cybercrime centres on online interactions. This is largely in

keeping with the idea of cybercrime as a bold new frontier. But in reality, and as has been discussed earlier in the introduction, cybercrime is simply another form of crime. Just as Reuter (1983) found that the often mythologised phenomenon of organised crime is far more localised and small scale than people realise, cybercrime is also inherently rooted in local settings. While a large amount of online activity takes place, many cybercriminals appear to know at least some of their collaborators in person. Such offline groupings have already been suggested in a number of publicly known cases, including that of Max Butler, the elite hacker and carding forum administrator. Butler's key partner, and the only person to fully know of the link between Butler and his online identity Iceman, was a fraudster called Chris Aragon who had met Butler offline through a mutual (criminal) acquaintance. While their relationship was not one of perfect trust, they were effectively bound to each other and engaged in extensive criminal activity together, until Aragon was arrested and turned Butler in (Poulsen 2011). In a similar vein, as was discussed in chapter 4, leading cybercriminal Albert Gonzales operated with a core group of associates offline as part of his activities.

Other publicly known cases suggest the existence of sophisticated organisations that approximate the structure of legitimate technology firms. Earlier in chapters 3 and 4, the Carberp case was discussed, where a malware group was operating together out of a physical office space (Ragan 2012). The Russian Business Network was an even bigger organisation, with a physical base in St Petersburg and connections to the broader Russian technology sector (Graham 2009, pp. 171-172, Krebs 2014, pp. 17-24). To understand the scale of what is possible for offline cybercriminal businesses, one need only look at the case of Liberty Reserve which was probably the most popular virtual currency used by cybercriminals during its operation:

> By 2010, Liberty Reserve was gaining tens of thousands of new accounts each month. The company soon looked the part of a successful tech start-up. It had more than 50 employees in departments including human resources, accounting, marketing, and legal, and provided around-the-clock customer service and technical support. Liberty Reserve's headquarters were in the same office park in San José, the capital [of Costa Rica], as branches of Hewlett-Packard, Procter & Gamble, and Western Union. The company housed its servers in the Netherlands and employed programmers in Ukraine. Its customers, of course, were everywhere (Halpern 2015).

The data collected for this thesis supports these suggestions of a strong offline dimension in relation to many cybercriminals. There are three main categories of this type of interaction: 1) meetings between individuals; 2) more formal gatherings often for a specific purpose; 3) offline groupings, a number of which should be considered firms, that operate together consistently over a period of time. First are those individuals who choose to meet as part of their ongoing business or even perhaps for social reasons. Within the sample, it was relatively common over time for some cybercriminals to grow closer with online partners, gradually exchanging some personal information and even phone calls (WE-(F)CC-1, NA-(F)CC-2, NA-(F)CC-3). The far end of this process involved meeting in person. This was relatively rare but still present. Scott was arranging to meet a collaborator who happened to be passing through town, but the meeting did not eventuated (NA-(F)CC-2). Lance had met at least one local collaborator, and even travelled to Eastern Europe to meet with some leading cybercriminals there. This was ostensibly a business meeting but he also wanted to "tool around". Ultimately he added, there's "always fraud committed" (NA-(F)CC-3). These meetings took place despite his belief that: "More often than not, and when I say that I mean 90 percent of the time - maybe 99 percent of the time

- you never talk to these people over the phone, you never go and visit them. We had a standing rule that that was one of the things you should not do: you should never agree to meet these people in person" (NA-(F)CC-3).

Ahmed, a former cybercriminal based in Southeast Asia met one of his collaborators, but the purpose was purely business in his case. Ahmed operated as a teenager and, among other activities, had hacked various websites for user data. He came to meet another user online and over time they chatted a lot and "grew close". Eventually this contact asked if Ahmed had any wares to sell and mentioned that he knew "a guy" who could use them. Ahmed's contact turned out to be from the same country as him and they arranged to met face to face to carry out their transaction, meeting in a cafe in a different town from where Ahmed lived (SEA-(F)CC-1).

The second form of offline interactions is gatherings of cybercriminals. Such events seem to be built around coordination and networking. As noted in chapter 3, the most famous of these events were the CarderPlanet conferences of the early 2000s. These meetings appeared to take a similar form to business conventions, or mafia meetings, allowing members from across the region and the world to meet, interact and discuss key decisions in relation to the enterprise. But while those large meetings have attracted a lot of attention, smaller meetings also took place. Within the CarderPlanet network, Fyodor made clear that a number of other gatherings occurred in the early 2000s. It was not the major conferences alone (EE-(F)CC-2). He wrote about a meeting he attended elsewhere in Ukraine, with an elite group of Eastern European cybercriminals, as a combination of business and pleasure:

> Anyway, Ukraine is praised for it's summer nights by Gogol and many other classics, and loved by folks looking for recreation and romance. It is no need to say that Ukrainian women one of most beautiful in world, Ukraine's politician - one of most stupid, and Ukraine's police - one of most corrupted. Nothing than such a combination is better for a "carder's" and that's what attracted us. We drove expensive cars ignoring any rules, drunk to coma, snorted coke and meth, and then danced to exhaustion, meet girls and had sex daily and nightly. It was good times, and there wasn't no one to stop us. If we didn't drank or got high, we met at some rented apartment with network of laptops and brainstormed some ideas, hacked for fun, or developed new methods or concepts (EE-(F)CC-2).

At this meeting, the group hacked a number of targets. Much of this was based around gathering information on companies and individuals that might be used in financially motivated attacks, but some was just for fun. Some of the ideas at this meeting were fully realised by the group at later times (EE-(F)CC-2). There are no known meetings of cybercriminals on this scale in the West. This could mean that the data has simply not been unearthed. But more likely, it is probably due to the enhanced enforcement and penalties facing those who might attend. If such meetings have occurred, they are most likely carried out in a much more subtle way than the Ukrainian meetings of the early 2000s.

The third form of offline interaction is operational groupings that carry out cybercrime together. Often these groupings take the form of firms. As noted in chapter 4, there are various online firms that engage in cybercrime together, distinct from forums which act as marketplaces for firms and individuals. But firms may also appear offline, and in some sense this is easier for their operation. In the case of Eastern European cybercrime, the CarderPlanet era might be defined by that forum and the meetings that took place, but in practical terms it was a number of firms

within that network that were actually carrying out the various attacks. Fyodor described these groups as being "somehow related but competing teams". Though some members may have moved, he named the key teams based on the geographical origins of their founders or most of their members: Odessa; Sebastopol; Donetsk; Kiev; Moscow and so on. In these cases, the groups physically met and worked together. While operating as distinct units, some of the key players in these groups knew each other and also attended meetings, like those discussed above (EE-(F)CC-2).

In other parts of the world, offline firms play a very important role. For instance, in Romania, online fraud has emerged as somewhat of a local specialty and a major regional employer. Relatively large firms there are well coordinated and operate out of apartments that they regularly change to avoid detection (ROM-LE-1). These groups became famous in the early 2000s for their expertise in online auction fraud, with eBay being a major target in the beginning. In short, they advertised and sold items online that did not exist, with discounted luxury cars being a particularly well-known hook in the early days. Over time, they diversified the scam and also targeted other sites like Craigslist and websites offering online accommodation rentals with the same central tactic of advertising a non-existent product (ROM-(F)LE-1).

While the scam seems relatively simple, the organisational structure behind it is not. Many of these enterprises are carried out by firms rather than individuals. These businesses operate out of the same physical spaces and have a clear hierarchy. There is the boss who oversees everything and the underlings who correspond with the victims and facilitate their payment. Depending on the scam, there may also be some

need for "tech support", which could involve assisting with the hardware, producing fraudulent documents used to enable the scam or designing phishing sites (ROM-(F)LE-1, ROM-(F)LE-2, ROM-LE-1). There is also a separate team of money mules known in this case as "arrows", who must transfer the money from the victim's country (or another location that is unlikely to raise suspicions) back to Romania. Each team of arrows is usually led by a trusted manager who recruits and oversees the mules. This role often has a degree of autonomy, perhaps even working with, rather than for, the central leader in Romania. In some cases, the arrow manager recruits only other Romanians in his area to move the money around, but in other cases he may also employ citizens in the country of operation or resident foreigners. But such arrow groups usually appear to be distinct from the firms that carry out the scams back in Romania (ROM-(F)LE-1, ROM-(F)LE-2, ROM-LE-1).[41]

While there is certainly evidence for offline cybercriminal firms, one must not get carried away and assume all offline groupings are firms. Sometimes it can be quite hard to distinguish between firms, outsourcing relationships and informal collaborative groupings. The Nigerian case bears some similarities to Romania in that there is a strong focus on online fraud with a significant offline dimension among the offenders. But in the case of Nigeria, some of this fraud is carried out by individuals, and the groups involved are generally more loosely structured. Nigeria became famous for what are known as 419 scams, named after the section of the Nigerian Criminal Code that deals with fraud. The central scam genus is also known as advance fee fraud, which involves the promise of sharing a larger amount of money

[41] There are also cases of cybercriminals from elsewhere in the world operating from different jurisdictions than their own. Sometimes this is to assist scams carried out locally or cash out operations in those jurisdictions. It is also relatively common for cybercriminals to move jurisdictions if they appear to be attracting too much attention from local law enforcement, or simply because they wish to enjoy their money (and the high life) in another location (RUS-CSP-3, RUS-(F)LE-1, EE-(F)CC-2).

(or valuable item) with a victim, if only they will pay a smaller amount in advance in order to unlock it. The scam has been tailored to address inheritance, packages coming through customs and job opportunities among a number of other schemes (NIG-(F)LE-1, NIG-CSP-1, NIG-LE-6). Nigerians are also known for romance scams, but this differs slightly in that the hook is a potential romantic involvement rather than a large sum of money. Advance fee fraud began in the 1980s and originally took the form of letters. But when the Internet came to Nigeria in the 1990s, the famous Internet cafes sprang up and provided locations where scammers could take their enterprises online and reach many more people. Later, as Internet access went mobile and into homes, cyber cafes became less of a feature (NIG-(F)LE-1, NIG-ITP-1).

Interview subjects regularly struggled to give a clear idea of how Nigerian cybercrime is organised, which gave support to the view that it is likely loosely structured without clearly identifiable hierarchies. There is certainly evidence of specific groups forming, but there was not strong evidence for tight, clear vertical structures. Participants are often made up of friends or others who have known each other for some time, through school, university or the local community (NIG-(F)LE-1, NIG-LE-6). But the groups appear somewhat informal, with membership shifting and new members joining to provide functions or services based on past relationships rather than being formally recruited. Sole operators also exist. It seems much more like a network of those working on similar subjects who share information and provide help as needed based on pre-existing connections (US-P-2).

While these offline groupings have a strong localised element, they also operate from

different jurisdictions. There are Nigerian fraudsters operating out of a number of jurisdictions around the world, including: the United States, the United Kingdom, the Netherlands, Dubai, Malaysia, India, South Africa and Ghana (MY-LE-3, US-P-2, NLD-LE-1, NLD-LE-2, UK-LE-2, US-LE-9). But rather than an octopus-like global conspiracy with a clear leadership committee, this network is more banal. It does not appear that individuals are actively sent to other locations to perform a role, but more likely happen to travel there for studies or other purposes and then seek to exploit the opportunities presented to them (NIG-CSP-1). In each location, they continue to operate as localised groups, even if they may work with others back in Nigeria (or elsewhere).

There are three common functions for Nigerian scammers to perform while overseas: 1) they may be there for training purposes in order to learn about hacking or computing in, for instance, Malaysia or India; 2) they may be offering a service that assists scammers back in Nigeria, such as coordinating money mules in victim heavy countries or purchasing goods with illicit proceeds (e.g. renting cars) that can then be shipped back to Nigeria; 3) they may operate their own fully fledged scams from their overseas bases (NIG-CSP-1, NIG-(F)LE-1). In this final category, it appears quite common for the Nigerians to incorporate locals into their scams. But this often takes the form of finding girlfriends who then assist their operations by helping to give the scams more local credibility (MY-LE-3, NLD-LE-1, NLD-LE-2). This may involve ensuring the scams refer to accurate information, such as the correct airport in a customs scam, or to answer phone numbers listed in scams with the appropriate local language or accent to appear more convincing.

Beyond the Nigerian case, there are other examples where the line between a firm and other types of offline grouping is less than clear. In the West, many of those who work on the money side of cybercrime often operate in relatively loose group structures. In some cases, they might be regular employees on salary. In other cases, the workers are on more of a freelance contract arrangement. For instance, Scott operated cash out crews, which involved him overseeing a number of offline contacts, who would withdraw cash from ATMs with counterfeit cards he provided. The workers would turnover quite regularly, and he didn't consider them his employees in a formal sense (NA-(F)CC-2). In another similar case, Sean made online purchases with stolen funds as part of his hacking enterprise. He required those who could receive the deliveries ("drops"), whereby the purchased products would be mailed to addresses given by these workers. While he later changed his system to handle more of the deliveries himself, he described his original system as more of a freelance affiliate scheme than a firm:

> From that point [when he had access to the stolen card details to make online purchases] I then either deal with the drop people, I called them drop girls because they were mostly girls, I dealt with the drop girls myself. Or I would have other people dealing with the drop girls for me, or arranging those contacts, kind of like referring them and I would give them something for doing that. Kind of like a referral/affiliate but in a very non-business manner. The deliveries would then go to the drop girls. They would then receive it. I would pay them per parcel rather than per item. The parcels would then come direct to me. I would give the person the money for referring, I would give the person the money for receiving the goods. Those goods would then go to an undisclosed location and then I would then get money from delivering them to the person it was to be delivered to. And there was never any sort of traffic back and forth (WE-(F)CC-1).

The final point to address with regard to offline groupings is that they do not need to

be entirely divorced from online interactions. Those that meet after establishing contact online first, clearly demonstrate this. But even in those instances where offline groups emerge out of local relationships, actors may also engage online if need be. This would usually be to interact with individuals who cannot be readily sourced through offline contacts. The Nigerian case provides a good example of this. Traditionally they operated largely within offline groupings and that still provides the core of their structure. But over the years, they have increasingly engaged with online forums as a means to access actors with greater technical expertise, either to hire services, buy tools or equipment, or to purchase data (NIG-(F)LE-1, NIG-CSP-1). Such activity has allowed Nigerian attacks to become more "sophisticated", but in reality they are simply piggy backing off the higher skill level found in Eastern Europe and elsewhere. Similar mixing of the online and offline can be seen in a number of other jurisdictions around the world, including Romania, Eastern Europe and the West.

Like many things in cybercrime, it's best not to look for a hard line separating different spheres - in this case offline versus online. The purpose of this section and chapter overall is to highlight the often overlooked offline aspects of cybercrime that play an extremely important role in the ecosystem. Cybercrime is not solely about a new online enterprise, much of it remains rooted in the traditional physical world, where its inhabitants live and go to sleep at night.

Why Offline?

There are a number of reasons why offline cooperation may be appealing to cybercriminals. One could start with the simplest explanation: that it's convenient and efficient to work with those in your vicinity who are already known to you. This certainly saves the time and effort of finding new partners online when you have a perfectly good pool of talent on your doorstep. But this explanation is really a manifestation of a desire for trustworthiness. It might be convenient and efficient to work with local contacts, but that convenience and efficiency are probably tied to the fact that these contacts are already trusted to a degree. It is not actually that inconvenient, for those with an interest in technology, to log into an open forum and either advertise for partners or to call on those who have already advertised their services. The true convenience offline lies in there being less need to vet one's collaborators because they are not anonymous strangers. The key element therefore becomes the importance of offline reputation in dealings.

So one could then move to examining trustworthiness as an explanation. There is some support for this, as it seems clear that many offline groupings originate or are sustained through existing offline social networks. Scott explained that his cash out workers were "recruited offline just by being friends, know someone that you can trust that wants to make some money and put them to work" (NA-(F)CC-2). Sean, who used drugs as a teenager, sought help from others in the local drug community to act as "drop girls":

> I had a lot of contacts from general drug taking and stuff like that and that's why I managed to get a lot of these people and of

> course, when you are taking drugs, the people have the same lack of respect for the law and that same lack of, you don't understand the consequences, or not caring about the consequences. That made it very easy to find new people for these drop addresses (WE-(F)CC-1).

In other contexts, a premium is put on working only with those who are well known or come recommended from a trusted contact. For instance, Romanians operating inside the country, and even some outside the country, choose to work with those who are well known to them from their local community. In fact, cybercrime in Romania appears in very specific geographic locations. Ramnicu Valcea has gained a reputation as Hackerville, but Fraudville would be a more accurate descriptor given their focus on auction fraud and other online scams rather than technical exploits (Bhattacharjee 2011). There are also other centres of fraud, including Alexandria, which predated Ramnicu Valcea as the cradle of cybercrime in the country. As law enforcement attention increased, some actors moved to Bucharest where is it easier to blend in, or even overseas (ROM-(F)LE-2). But the small town origins of the phenomenon suggest the sort of close links and neighbourly relationships that might approximate kin relationships and serve as a solid base from which to derive successful cooperation. In the Nigerian context, actors also appear to work with those whom they have known well for some time, often living in the same community, if not attending the same school or university together (NIG-(F)LE-1). Strong bonds appear to matter.

Something similar may also apply to those cybercriminals who connect with collaborators online and then later decide to meet offline. When asked directly why someone might take the risk of meeting in person, Fyodor's answer was somewhat

ambiguous:

> Well. Maybe because they stupid? Careless? Dealing with the people is normal. And some people want to go beyond the screen and keyboard. This is a flaw, a flaw of human nature. Or is it a flaw? (EE-(F)CC-2)

But his further elaboration on these issues offered some clearer sense of motivation: “Sooner or later people normally getting close, trusting, and naturally want to meet, because "life stories" is the part of online business, and people tell how they are, bragging, sharing and finally want to meet each one other in real life” (EE-(F)CC-2). In short, they want to get a better sense of who they are dealing with. Actors will usually only meet with those they have known for sometime online and have some trust in already. In the cases where Lance physically met with his collaborators he had done “so much” business with them that he “knew these kids had nothing to do with law enforcement” (NA-(F)CC-3)

Whether offline interactions take place between online contacts or with those already known in the community, it appears that trustworthiness plays an important role. Those who work with members of their community are trying to draw value out of their existing social relations. By working with relatives, friends and others in the local community, offline cybercriminals are exploiting trusted relationships that may already exist. They have a history of past interactions with those already known to them, which as we saw previously increases trustworthiness. This might offer a stronger alternative than making contacts online, even those with whom a chain of interactions can be successfully built. On the other hand, those online contacts who choose to meet in person may also be seeking to better verify and vet their partners in

person. The desire to meet with partners is likely due to the inherent instability of dealing with anonymous online partners. Only by learning someone's physical identity can you gain a better sense of who they are: how trustworthy someone might seem online can be supplemented with offline elements of their reputation, appearance and performance, to paint a clearer picture. And only by revealing your own identity can trust be more firmly established between various actors. When collaborators have been identified physically, it reduces the risk that a partner might simply vanish.

But the importance of identity moves beyond reputation and essentially links this discussion to enforcement. The chief significance of a physical identity is that you can locate the person if need be. If trust is breached, the person can be found and punished accordingly. Prior to that, his activity can be more closely monitored to avoid defection in the first place. In such cases, the sanction can be social rather than violent. One famous example of this is cooperation among diamond traders, and specifically the Orthodox Jewish traders who play a key role in the New York City wholesale diamond market. In this case, diamonds of great value are passed to potential buyers for private inspection as part of a sale, without insurance against the theft or replacement of the diamonds with counterfeits. Coleman notes that the close ties held by many in this business essentially lead to a closed community: the traders belong to the same religion; live in the same parts of Brooklyn; attend the same synagogues; they regularly intermarry between families (Coleman 1988, pp. 98-99). Coleman provides this explanation as to how this market can sustain itself without any formal insurance mechanism:

> Observation of the wholesale diamond market indicates that these close ties, through family, community, and religious affiliation, provide the insurance that is necessary to facilitate the transactions in the market. If any member of this community defected through substituting other stones or through stealing stones in his temporary possession, he would lose family, religious, and community ties. The strength of these ties makes possible transactions in which trustworthiness is taken for granted and trade can occur with ease. In the absence of these ties, elaborate and expensive bonding and insurance devices would be necessary – or else the transactions could not take place (Coleman 1988, p. 99).

While diamond trading is a legitimate business, cooperation among cybercriminals may not be much different. This aspect of enforcement helps explain why cybercriminals might choose to work with those known to them offline and those with closer ties are likely to make more successful collaborators. Campana and Varese have argued a similar point with regard to broader criminal settings and kinship specifically. They suggest that: "if the member of the crime group still decides to defect on his associates, the latter would be able to find him and his relatives more easily if he shares kin ties with other members. In effect, both he and his immediate family are hostages of the larger criminal group" (Campana and Varese 2013, p. 281). The same line of thinking should apply more widely to close relationships beyond kinship, and it would seem logical that a spectrum of the intensity of ties would predict the effectiveness of insurance against defection. The sanctions involved could be violent, but also purely social.

As a result, working offline and providing parties with a knowledge of one's true (physical) identity acts as a credible commitment. This could be viewed in terms of cutting off options: once one's involvement in cybercrime is known, one can't easily retreat back into online anonymity. Nonetheless, Schelling's concept of information

hostages probably offers the closest fit. At this point it is useful to quote Gambetta again from the introduction, in relation to online paedophiles meeting offline: when "identification is at a premium and must be kept secret, just showing one's face is itself like giving a hostage, namely the knowledge of one's key sign of identity" (Gambetta 2009a, pp. 62-63). This applies very much to the case of profit-driven cybercrime as well. The more one knows about a collaborator, the closer they are bound together and the easier to enforce agreements. By interacting offline, cybercriminals open up, and open themselves up to, traditional tools of physical enforcement among criminals: threats; destruction of property; harassment; beatings; torture; death. Such enforcement avenues, coupled with a knowledge of offline identities, lower the risk associated with defections in cybercriminal dealings.

The remaining paragraphs in this section examine some of the specific tools of enforcement that are evident in the data. It focusses on violence, monitoring and social sanctions. In discussions of traditional forms of crime, violence often appears as a key enforcement tool. Ostensibly, the online dimension of cybercrime offers a new frontier where violence is no longer an option and other avenues for enforcement, or other mechanisms to enhance cooperation, need to be developed (see chapter 6). But that narrative only holds true if cybercriminal activity is focussed online. In offline settings, the spectre of violence reemerges. Probably the most famous known example of violence by a cybercriminal was the kidnapping and torture by the Turkish cybercriminal Cha0 of a hacker known as Kier (Singel 2008). There are claims that the hacker was beaten and threatened at gunpoint for informing on Cha0's group. Cha0 posted a picture of Kier online in his underwear commemorating the occasion, but most likely aimed at embarrassing Kier even further. Kier was holding a sign:

I am Kier
My real name is:
Mert Ortaç
I am partner of the media
I am rat. I am pig.
I am reporter.
I am fucked by Cha0[42]

In a sense this is like an extreme form of *doxing*. *Doxing* online could have revealed Kier's real identity, but by kidnapping him and providing his true, physical, identity the shame is even greater. It sends an even stronger message to both Kier and others. But such an attack could only be carried out because those involved were physically known to each other and was helped by the fact that they all lived in Turkey. It illustrates what offline relationships allow in terms of increased enforcement. Cha0 had mooted connections to both organised crime and corrupt Turkish government officials, but his view of himself as somewhat of a hardman suggests that more serious forms of violence, even homicides are at least a theoretical possibility in cybercrime (US-LE-2).

Throughout interviews for this project, a number of instances of violence were recounted. Sean mentioned that violence was an option when dealing with his offline contacts. He noted that there was one occasion where he had to: "give someone a little bit of a seeing to because they were fucking me around. But that was only very light, just going around there with someone else just saying what's up, where's my money kind of thing" (WE-(F)CC-1). Ilya knew of a case where an arrangement between a group of Russian hackers and a company that was using their services had gone awry. With the company refusing to acquiesce to the cybercriminals' demands, the group

[42] The photo can be viewed at: https://www.wired.com/2008/08/hacker-reported.

returned with baseball bats and unleashed on the office. He described this type of individual as being smart but with a liking for violence – a very dangerous combination (RUS-CSP-8). Igor described many of those involved in Eastern European cashing out operations as "real criminals" who are dangerous and one must be wary of them (UKR-CSP-3). In the Nigerian context, former law enforcement agent Idris claimed he had heard of cases where cybercriminals killed each other. Knowledge of where a collaborator lives can be very helpful in this regard: "The penalty for breach of trust is death" (NIG-(F)LE-1). Violence has also been made mention of in other contexts, such as Romania.

Despite these instances, it is important not to depict cybercrime as extremely violent. While the threat of violence becomes available through offline interactions, it is not always acted on. Violent episodes among cybercriminals appear to be less common than in some other forms of crimes, such as within traditional organised crime activities. The next chapter will discuss aspects of organised crime involvement in cybercrime, and the violence that can come with it. But in a number of instances, it appears that cybercriminals themselves actively seek not to involve themselves in violence. Scott never employed violence in his dealings with cash out crews. He simply stopped working with a person if they were scamming him too much (NA-(F)CC-2). Several current and former law enforcement officers across a number of jurisdictions including Eastern Europe and Nigeria reported rarely, if ever, seeing instances of violence among cybercriminals (ROM-(F)LE-1, NIG-LE-6). In many instances, whether the crimes involved were highly technical or not, those centrally involved in cybercrime were described as being "smart" guys. These are the types of actors who appear more willing to use their brain than their brawn.

While violence, or the threat thereof, plays some role, there are other tools related to enforcement that the offline dimension also allows. Foremost among these is increased monitoring opportunities. The way arrows are overseen by their Romanian managers is a good illustration of this. As the final part of scams, the arrows are responsible for withdrawing/transferring money and they are the most at risk of arrest. But their manager does not simply trust that they will do as they are told and not run away with the funds. According to Romanian law enforcement agent Alexandru, a manager will wait nearby, watching what is happening to ensure things are done as they should be (ROM-LE-1). While this is short of actual violence, it suggests a degree of supervision and perhaps threat that is likely to encourage greater compliance among the arrows. In the North American context, Scott also monitored his cash out crews, but he employed a different method, rather than shadowing his operatives everywhere:

> As far as trusting them not to steal from you, you just have to give them a test run and if things don't add up on the results when they are done and you feel like they are screwing you, you just cut them off and tell them things are not working anymore or whatever. It is expected though, in my experience, that almost always they all end up eventually stealing a little more and more as time goes on, but usually I didn't have any way to prove it for sure or I just didn't care enough to try because it wasn't enough to make a difference in profits. I had done some recon here though and kept tabs on what they were doing without their knowledge just to see. For example I have done the same thing with THEIR emails/phones whatever and also I had actually slipped in some prepaid greendot cards[43] in batches that I paid for and had online access too etc to see if they tried to say it didn't work when I know it did etc and if I did find them being un-honest (lol funny huh, un-honest criminals?) then I would slowly just phase them out. What else can you do? (NA-(F)CC-2).

[43] A form of prepaid Visa or Mastercard cards.

As with his online dealings, Scott demonstrated a degree of acceptance that he would never achieve full cooperation from his workers. As noted above, he would not resort to violence, but would simply cease cooperation himself. This was not a perfect system, but a functional one that relies on close monitoring in order to weed out defectors.

In other cases, the offline dimension provides an opportunity for monitoring specific transactions rather than overall group activities. As noted above, Ahmed connected with a collaborator online but later physically met with him in cafes for the purpose of transactions. He now looks back on those interactions as risky. He remembers being scared at various points as he was dealing with an older contact and was also on edge whenever he saw police. When asked why he did not simply carry out the transactions online, he argued that he would have preferred not to have to meet, but that his main concern at the time was to ensure that the money was paid for the goods and also that he didn't leave an electronic trail. He thought it was best to physically exchange the CD with the relevant data on it, directly for cash (SEA-(F)CC-1).

Finally, social sanctions can also play an important role alongside violence and monitoring. The discussion above on this topic illustrates the manner in which this would work in close-knit communities, where offenders are well known to each other and live in the same neighbourhoods. Those who defect are shunned not only by their collaborators, but by the broader community as well. The tighter the community, the more damaging the sanction. Rather than delving further into this somewhat standard manifestation, here I address one of the more unusual social sanctions that emerged over the course of this study: voodoo. In certain parts of Africa, including Nigeria,

there is a fairly widespread belief in voodoo, known locally as *juju* (Aguazue 2013, Tade 2013). Aspects of *juju* have taken on some importance for a range of Nigerian criminal groups, including human traffickers. In these groups, *juju* can be used in a number of ways, including to curse victims or their families as a threat and substitute for violence (Baarda 2015). But *juju* has also become important for cybercriminals. Some aspects of the belief are rather perfunctory. They involve rites before shrines, where appeals to spirits are made to achieve success in cybercriminal scams. Some payment must be made to the spiritual leader and the ritual might relate to a specific email that will be sent (NIG-LE-1, NIG-LE-2, NIG-LE-3, NIG-LE-4). In basic terms, the invocation of *juju* is hoped to enhance the duping of victims.

But there is another aspect of *juju* that relates directly to cooperation. Just as human traffickers use *juju* as a substitute for violence, so too do cybercriminals. But in the case of cybercrime, the subject of this substitute for violence is not victims but collaborators. Idris explained that cybercriminals swear oaths to be part of a group and not to betray them. The oath is the "first layer, the second layer is the violence". But the oaths themselves are perceived by *juju* adherents to be a physical threat and possibly deadly. Idris suggested that cybercriminals believe that if you swear an oath at a shrine and break it, then you will die (NIG-(F)LE-1). Gideon, who works in the Nigerian technology sector but is involved with investigations, also suggested that oaths were important among cybercriminals. He agreed that there are beliefs that breaking an oath is deadly and claimed that this can even lead to defectors going into convulsions. Gideon argued that these religious elements are the "critical factor" that maintains cooperation in these groups and prevents many from informing on other group members. They would prefer beatings and the threat of gaol over breaking their

oaths (NIG-CSP-1). This certainly seems a novel addition to the famous prisoner's dilemma scenario.

Failures of Cooperation

While the offline dimension offers a number of advantages in terms of enforcement, there are obviously cases where cybercriminal cooperation still fails. It is valuable to study these failures in the offline setting, as another way to incorporate variation and not select on the dependent variable. In the case of Sean's drop girls, there were a number of problems and he eventually moved to a different system that was largely self-managed. The failure of using local people in his drug community was directly tied to their drug use. What made them an available pool of criminal workers happy to break the law, also made them a risk to work with: "The problem was with that, there was a lot of distrust in that. And I can recount quite a few occasions where people had said oh an item had not turned up when it clearly did and they were just trying to pull a fast one" (WE-(F)CC-1). Scott had similar problems with his cash out crews, where he believed most would deceive him at some point. He was willing to accept such defections as the costs of doing business (NA-(F)CC-2). But Sean went on to explain that his workers' unreliability went beyond scamming him into problems with law enforcement:

> That model fell apart. I explained in explicit detail to these people how not to get arrested and how to make sure you get released within those 72 hours of being arrested. And that is to say absolutely no fucking comment all the way. Don't say a single word, they cannot prove anything. Unless, if they ask you, just say I was just signing something, someone asked me to sign something for them, I didn't know what it was, I was just doing them a favour, I didn't know anything, I didn't

> realise I was doing anything illegal. That is the story to stick to. Either that or no comment. And then you'll be fine. But these people didn't realise that. But of course when you get arrested, I kind of assumed they would have the same hardened approach that I would have, and of course they didn't. Leave them in a cell for 12 hours to think about what they are doing and a lot of people will crack after that amount of time. Whereas if it's me, I would just sit there, go to sleep, wake up and oh interview time already? So that was my biggest flaw in that (WE-(F)CC-1).

This experience led Sean to come to the sad realisation that "People are dumb" (WE-(F)CC-1).

These examples are best contrasted to the Nigerian and Romanian contexts where cooperation appears to be relatively successful. The key variation between these cases and the failures discussed just above is that a premium is put on working with trusted contacts who have been known for some time. In both Romania and Nigeria, collaborators appear to come from the same towns or neighbourhoods. Some have familial connections or have been educated together. In one case in Romania I encountered, law enforcement agents began an investigation and eventually discovered that almost an entire village was involved in the illegal enterprise. This contrasts with the cases above where workers are chosen much more opportunistically. Sean wasn't drawing on a close-knit community with strong ties and extensive social capital. He was working with people whose situation as regular drug users made them inherently untrustworthy. In fact, he later changed his system to become almost entirely reliant on himself, the most trusted person in the equation. Scott appeared to take some care with those that he worked with, but the bonds did not appear to approximate those in communities elsewhere. He was not working with close family or friends.

The overall point to be drawn from these examples of variation and cooperation failure is that, the closer the relationships, the more likely it is that successful cooperation will take place. Dealing with weak offline ties has some similarities with dealing with strangers on the Internet. There may be limited information on their true identities, where these individuals live and their social circles. This creates difficulties not only in terms of reputation but also enforcement. It becomes much more difficult to adequately monitor collaborators and take action if need be. Social sanctions are also likely to be less effective. Defections still take place in the Nigerian and Romanian contexts, but at least anecdotally the model of dealing with more closely known and vetted individuals seems to be a more successful one (ROM-(F)LE-1, ROM-LE-1, NIG-(F)LE-1, NIG-LE-6). As such, the cases of failed cooperation appear to support the idea that greater enforcement is what the offline dimension really adds to cybercriminal cooperation.

A Balance Between Online and Offline?

The above sections have argued that there are strong incentives for cybercriminals to operate, at least to some degree, offline. US law enforcement agent, Ethan, sums up the situation in terms of the higher levels of trust that can be garnered through offline interactions and the risks that can come from online interactions:

> And I know for a fact that people will fly. They will travel to meet each other to talk in person. And many times - and I've had personal experience with this – people only want to communicate via mobile phone now. They only want to communicate via text message over phone. They don't want to get online because the perceived risks of even getting online to communicate... bad actors understand that they're just increasing the risk overall by doing that. So I think for them anytime they

> communicate over out-of-band channels, and mobile phones are really out-of-band channels, but when you talk about the majority of bad actors and the way they communicate most of them use the Internet. So I've personally seen a lot more of what I call high-level players only communicating with people they know. They've met in person. They have a phone number for. But I couldn't give you a specific example of a sophisticated malware campaign with any longevity that was operated by multiple players that were really globally-dispersed, and they had never met each other (US-(F)LE-1).

This idea was echoed by Ilya, a Russian security researcher, who argued that some of the leading cybercriminals in Russia strategically try and keep an offline-only presence. They realise the inherent risk of leaving digital traces through online interactions (RUS-CSP-8). This can become evidence that later ties them to a crime. This digital evidence simply will not exist if they only engage with their offline confreres.

But of course, not all see matters in the same way. For many discussed in this chapter, a combination of online and offline interactions is key. As in Ahmed's case, cybercriminals might operate largely online and then seek to meet in certain key moments. In other cases, there might be a strong offline structure that allows the group to function effectively, such as Fyodor's elite "teams" spread throughout Eastern Europe. But in such cases, online interactions allow these groups and individuals to expand their contacts and partner with individuals in other locations. As noted above, the Nigerian case provides an interesting example in this regard. Many Nigerian cybercriminals operate with those personally known to them. But in recent years they have been increasingly going online and doing business on forums. The key reason for this is that they can access products and expertise that they cannot obtain from within their local community. Online they can engage with Eastern

Europeans and others to purchase card data, malware or perhaps learn some new skills themselves. Rather than being a counterpoint to the offline dimension, in this case it is complementary.

On the other end of the extreme are those that choose to operate solely online. In such cases the risk of going offline is deemed to be too high. This could be due to the threat of arrest or simply a fear of other criminals they might do business with. Operating from one's home certainly brings a degree of safety. Along these lines Lance argued that: "the anonymity that is provided by being online, enables a lot of these people to commit crime whereas they would not have committed crime if they had to show their face to other people" (NA-(F)CC-3). In these cases, the ability to remain anonymous allows and expands the number of instances of cybercrime.

The approaches that cybercriminals take are likely very much tied to the contexts within which they operate. In the West, outside of cash out groups, offline collaboration is increasingly rare (US-LE-2). For many, a key rule albeit sometimes ignored, is not to meet in person because this is viewed as unsafe. Anonymity is what protects them from arrest (NA-(F)CC-3). But in other parts of the world where law enforcement capacity is lower and/or corruption levels are higher, offline groupings appear much more likely to occur. In those instances, going online and interacting broadly with other cybercriminals is more risky because this may put an actor on the radar of Western law enforcement agencies. But as law enforcement efforts improve in these regions, cybercriminals must also act more cautiously. It's perhaps no surprise that even in Eastern Europe, cybercriminals would be extremely brave to hold conferences like those in the CarderPlanet days. As outlined throughout this

chapter, smaller gatherings, groupings and firms still exist. But with increased attention from both local and international law enforcement agencies, careful operators have retreated further underground.

Conclusion

The offline dimension of cybercrime is central to the success of the industry. It appears to overcome some of the deficiencies involved in online interactions alone, namely the residual distrust that remains despite the steps taken by cybercriminals to address this challenge. This chapter provided evidence for this aspect of cybercrime, along with an explanation for why this type of physical collaboration occurs. Virtual cooperation has limits: online firms are generally small and short-lived. Meanwhile, the offline dimension allows for far larger, more sophisticated, stable and enduring structures. This element of cybercrime appears curious at first, but there are logical explanations for this, most notably the increased enforcement, through the threat of violence or other sanctions, that is not possible in a virtual world. While it brings its own risks, this type of offline activity ostensibly corrects deficiencies that come from operating as a faceless user. Anonymity protects identities, but also makes it much more difficult to maintain cohesion among larger groups. Online institutions and a degree of governance allowed cybercrime to grow from small-scale interactions to large marketplaces with thousands of members trading together. But the larger firms, some of which provide fundamental "infrastructure" to the broader industry, only appear possible when rooted in the physical world.

This chapter also addressed failures of offline cooperation, and how most

cybercriminals make use of both online and offline dealings. Ultimately, there is no perfect equilibrium with regard to how cybercriminals approach the online/offline conundrum. Some collaborate exclusively online, others almost exclusively offline. Many operate in a spectrum in between, seeking the types of cooperation that best suit their needs within the context that they operate in and the goals they seek to achieve. In some situations, like cashing out operations, offline collaboration is almost a necessity. In many other situations it is a choice. Each approach brings its own form of risk: whether of being scammed, arrested or otherwise.

The offline cybercriminal firms, and the exchange that takes place between these firms and individuals outside of the Internet, should not be that surprising. Just because cybercriminals have the option of solely engaging in online dealings does not make this a *fait accompli*. This so called offline dimension is simply how other financially motivated criminal enterprises have always operated, whether in the drug trade or other organised crime ventures (Levi 2008, Reuter 1983, Paoli, Greenfield, and Reuter 2009). This is not to mention the parallels between these cybercriminal businesses and some legitimate companies operating in the technology sector. As in the case of Liberty Reserve, apart from tailoring their services to criminal customers, there was little separating the operations of this payment processing company from a number of other start-ups. Of course, much of this ties into local law enforcement capacity and pressure. Cybercriminal firms are much more likely to expand and take on the appearance of larger legitimate enterprises when they are not being harassed by law enforcement. If they operate in grey areas of the law, shield their true dealings, or bribe the right people, success may follow and the industry will flourish even further. Aspects of this will be discussed in the next chapter.

8. Cybercrime, Organised Crime and Governance

Criminal markets benefit from order in the same way as legitimate industry. But while licit companies can rely on contracts and a legal system to enforce them; criminal firms and individuals cannot. Ultimately, the state protects the private sector and ensures that chaos does not reign, but, once outlawed, illegal activity cannot be regulated by the state any longer. As such, distrust can take hold in these markets. In such instances, there is a strong demand for institutions and governance, which must be met through alternative means (Dixit 2004). In a surprising number of cases, groups operating outside the state's formal control find avenues for extra-legal governance. This is the case among street gangs, prison gangs, pirates, mafias and more (Densley 2013, Skarbek 2011, Gambetta 1993, Shortland and Varese 2014). In chapter 6, we saw that cybercriminals have succeeded in establishing online institutions that promote trade, regulate the market and provide aspects of enforcement. The argument of the present chapter is that there is also a system of governance that supports the offline dimension discussed in the last chapter. This offline governance is essential to the successful functioning of the cybercrime industry.

There are three possible ways that offline cybercriminals could be governed. First, it's possible that certain cybercrime firms could have evolved to the level where they seek to monopolise the business and effectively take control of all relevant cybercriminals in their territory. Second, cybercriminal governance could be provided by organised crime groups, who arbitrate disputes, mete out punishments, drive out competitors and

protect cybercriminals from arrest. In the criminal underworld, governance is commonly provided by OCGs. As noted in the introduction, some even define organised crime as groups that seek to govern a criminal market in such ways (Schelling 1971). It is conceivable that these groups could apply the skills they have developed regulating other markets to the cybercrime industry. Finally, this role could also be performed by corrupt government agents. This category is not the state reasserting control over a criminal market, but rather individual state agents performing this function counter to their official role. Around the globe and throughout recent history, it is not uncommon for corrupt agents to carry out this function in return for illicit payments. For instance, prior to the rise of the mafia in New York City, it was corrupt police officers who primarily protected prostitution and gambling (Varese 2011, ch 5).

The organic development of a cybercriminal group capable of carrying out governance is theoretically possible, but found virtually no support in my data. As discussed in the previous chapter, there are some instances of violence on the part of cybercriminals, but they don't reach the scale and intent required to be classified as attempts at broad control of the industry. Possibly the closest example to this is found in Brian Kreb's book *Spam Nation.* Krebs recounts the early history of the famed Russian Business Network and a rare instance of violent behaviour between cybercrime competitors. At the heart of this history is Alexander Rubatsky, a talented programmer who became involved in a number of aspects of cybercrime, including payment processing for child pornography. His story has been mentioned a number of times throughout this thesis. Rubatsky ran a team of hackers to assist his operations, but was also supported by a group of heavies who provided a form of protection

(Krebs 2014, pp. 17-24). Krebs describes how the group dealt with a rival businessman named Evgeny Petrovsky who was developing his own credit card processing business focussed on child pornography:

> Petrovsky was stopped in his car by a man posing as a local policeman, and when he stepped out of the car as directed, he was kidnapped by masked men. Once they reached their safe house in the outskirts of Minsk, the abductors contacted Petrovsky's associates and demanded a million U.S. dollars for his safe return. But no money would be forthcoming. When local authorities began to close in on location, the assailants fled with Petrovsky to Moscow. By November 2012, Russian and Belarusian authorities had located the Loginov gang's hideout and the rest of the kidnappers. They found Petrovsky alive and relatively unharmed (Krebs 2014, p. 20).

This rare account is suggestive of cybercriminal governance but falls short. What is telling in this case is that the group does not appear to be a cybercrime group that has developed organised crime functions, but rather an alliance between a group of hackers and a group of heavies that was associated with the Belarusian OCG known as "The Village" (Krebs 2014, p. 18). While it's theoretically possible that a cybercrime group might evolve into an OCG, empirically it appears more likely that a traditional organised crime group will become involved in the business in some way. Or else, corrupt agents may play this role. It is these two elements that are the focus of this chapter. I investigate the role that each plays in governing the cybercrime industry and which group is more centrally involved.

Cybercrime and Organised Crime

There is a strong sense in blogging and media circles, along with some in the

cybersecurity sector, that organised crime is "taking over" cybercrime. There is a variety of hyperbolic quotes and statements on this subject, including that: the "Mafia, which has been using the internet as a communication vehicle for some time, is using it increasingly as a resource for carrying out mass identity theft and financial fraud" (Blau 2004). Others also prescribe a central role to the Russian mafia in particular: "The Russian Mafia are the most prolific cybercriminals in the world" (Goldman 2011). But strong empirical evidence is rarely provided on these points. Unfortunately, the issue is not dealt with in a much better fashion by the academic literature with a distinct lack of data and some loose claims (for similar arguments see Wall 2014, McCusker 2006).

As McCusker (2006, p. 257) notes, there is a theoretical tension over whether traditional organised crime groups are likely to involve themselves in cybercrime. On the one hand, if there were new opportunities to make money, one would expect traditional organised crime groups to take advantage of them. On the other hand, these groups may be satisfied by sufficient opportunities in their existing activities and do not need to engage in cybercrime, or else there is a technical barrier which may prevent them from doing so. This technical barrier is an important point. Despite popular perceptions of global criminal masterminds, many mafia members are "street guys" who specialise in violence and toughness and are far from worldly, often having tight links to their local neighbourhoods. The undercover FBI agent Joseph Pistone, who infiltrated the Bonanno crime family in the 1970s, provides an account of how some mobsters didn't even know how to book their own airline tickets (Pistone 1987). While technology is becoming increasingly widespread and is now likely being used by certain organised crime members, especially the younger

generations, the inherently localised nature of much organised crime should not be forgotten. This was one of the key findings of Reuter (1983) in his classic study *Disorganized Crime*.

Moving past loose claims and theorising, the rest of this section addresses what can be said empirically on the question of whether OCGs are governing cybercrime. Many participants in this study believed that organised crime involvement in cybercrime was substantial. But when pressed, this appeared to be a theoretical rather than empirical view. A common formulation was that organised crime moves to where the money is and the money is now in cybercrime. So that is where, logically, they would involve themselves. But when participants were asked whether they had directly seen a case of a traditional organised crime group involved in cybercrime, relatively few answered affirmatively. Many of those who had seen such cases, often described only a small number and/or provided limitations on their involvement. As such, the data collected for this project suggests that organised crime does play a role in cybercrime, but that its involvement is far from a complete takeover.

On the core question of whether organised crime groups are moving into cybercrime and supplying protection, there is some evidence but it is not overwhelming. Like any other criminals, if cybercriminals make large amounts of money they may become vulnerable to theft/extortion, both from the criminal community and corrupt law enforcement. If they are collaborating in their enterprises with other local (cyber)criminals, they may also require arrangements to be enforced by a "trustworthy" local mobster. The need for protection appeared to be at the heart of Rubatsky's early days in Minsk discussed above. When he later fled to St Petersburg

and eventually formed the Russian Business Network, there was again a need for a "roof" in the local Russian mafia (Krebs 2014). Of course, RBN was also well known for having a roof in law enforcement and political circles as well, which will be discussed in the second section.

While my data suggested some instances where traditional organised crime groups provided protection to cybercriminals, this was not the norm. In fact, there were many instances where this did not occur. In Romania, former law enforcement agent Virgil knew of groups that carried out protection rackets that made contact with cybercriminal groups. There were also cases where cybercriminal groups stole money from each other. But these behaviours were rare, with many groups being somewhat friendly with each other and having no real need for protection (ROM-(F)LE-1). In Nigeria, Idris also believed that it was very unusual for cybercriminals to be paying protection racketeers (NIG-(F)LE-1). Former Ukrainian law enforcement agent, Nikita, suggested that connections between Eastern European cybercriminals and mafia groups were usually more service based rather than built on protection (UKR-(F)LE-2). Former cybercriminal Fyodor also did not believe there was an especially strong association between cybercrime and Eastern European organised crime, writing:

> All the relations between traditional mafia and gangs are eventual and personal, so there's no more connections than in any other industry or enterprise. Some individuals do, and if they do, they use it. Others don't. There are various individuals with different backgrounds, some came from "IT" world to carding, other from world of crime. Of course, regular criminals show interest in certain aspects of cybercrime, but they show interest in many other things. More advanced carders and hackers, however, usually show strong disgust to "traditional" criminals and usually join whatever cause there might be on

> temporary basis. In turn, "traditional" criminals often regard cybercriminals as "milk cows" and nerds (EE-(F)CC-2).

Much stronger empirical support was actually found for the involvement of organised crime groups in cybercrime outside of providing protection. In other words, rather than seeking to govern cybercrime, those organised criminals who became involved in the industry were much more likely to play a role within it. Outside protection, the second role organised crime groups play in cybercrime is by acting as investors in certain enterprises. This requires little specialist knowledge from the organised criminals involved. They only need to make contact with a cybercriminal group and have a pool of capital that it has available from its other operations. In practice, my data did not suggest too many pure instances of investment, but it did happen. Perhaps the best example was provided by former UK law enforcement agent, Peter, who recounted a case of a group involved in credit card fraud, which he described as being on an “industrial” scale. The information on the case was sensitive so, according to Peter’s wishes I provide limited details here. The scheme involved hiring a programmer to develop software to access the card details from banks, and there were significant upfront costs for this. As a result, Peter believed the boss of the group sought the backing of a well-established British organised crime group to bankroll the operation. But following a falling out, the cybercriminal’s life was later threatened by them and he had to go on the run (UK-(F)LE-4).

The third role that OCGs play within cybercrime is to use their traditional expertise in money laundering and their ability to physically enforce group arrangements as service providers to, or partners of, broader cybercrime operations. The money side of cybercrime is the part that often requires offline groups of people to collect/send

money or buy merchandise with stolen proceeds. While there are many instances of this activity being carried out by groups that are not connected to traditional organised crime (NA-(F)CC-2), monitoring/enforcing this process is a plausible point of organised crime involvement. The collected data confirms this supposition with OCGs somewhat regularly appearing within this role. Perhaps the most famous case of this was the Citibank hack of 1994 involving Vladimir Levin who managed to infiltrate the bank's networks and arrange for a number of illicit money transfers worth millions of dollars. According to Nathan, a former US law enforcement agent, it was the Tambov Gang, a leading Russian mafia group in St Petersburg, which was responsible for overseeing the movement of the proceeds back to Russia. This involved a network of people in different countries around the world to receive and move the money. The gang made use of coercion and threats of violence to enforce compliance, particularly when the arrests were made. In one case, they paid the legal fees of an arrested member of the group. In another case, they attempted to murder a gang member whose wife had been arrested and was considering cooperating with the authorities (US-(F)LE-5).

Other examples also show OCGs adapting to meet new opportunities in dealing with monetary aspects of cybercrime. In these cases it is common to leverage existing resources within the group but for new purposes. The example of L.A. street gangs is particularly instructive in this regard. Such groups have evolved to include a fraud faction within their hierarchy (US-LE-1). Similar occurrences have been observed elsewhere in the United States like New York and Texas (Hong 2016). The way these enterprises work is a direct offshoot of the gang's existing hierarchy. As US law enforcement agent Lucas outlined, one gang member acts as the "fraud pimp" and

manages low-level runners (US-LE-1). The pimp's role includes buying compromised credit/debit card details online and overseeing an operation that manufactures the counterfeit cards. This offers a point of connection with the online world of cybercrime, as the logical place to purchase card data is on forums that are populated by cybercriminals from across the world. Here gang members can learn aspects of cybercrime and purchase the goods and services they might require. In fact, Lucas recounted amusing broken conversations that he observed online between Eastern European cybercriminals and American gang members whose use of language and approach to the business offered an interesting contrast (US-LE-1). Once the card data has been purchased and the physical cards have been manufactured, the fraud pimp then distributes the cards to two lieutenants who will arrange the cashing out. The split heavily favours the pimp who often takes around 90% of the profits, with the lieutenants performing their role for surprisingly little. A cut also has to be paid upwards to the gang's leadership (US-LE-1).

What is most interesting about these operations is the use of existing resources within the gang. The key actors in the cash out crews are women who might otherwise have been sent out for "tricks" (US-LE-1). It is a shift from a prostitution model to a fraud model, using the same individuals. While a trick might lead to $50-100, switching to cashing out might net close to $1000. The products purchased by these cash out crews appear to vary depending on the geographical base of the gang. Monthly passes for the Long Island Rail Road were popular for New York gangs, while Walmart was a prevalent target in Texas and Apple products were commonly sought by gangs in California. These products can then be sold on as in conventional fencing among

criminals. Lucas suggested that such street gangs carry out this fraud alongside their traditional operations such as drug dealing (US-LE-1).

The fourth role that organised criminals play in cybercrime is by directly getting involved and acting as the guiding hand of certain operations. This usually involves recruiting those with technical skills, among others, to carry out the jobs. One of the best examples of this phenomenon was the failed Sumitomo heist in 2006 where £229 million was almost stolen from the bank. In this case, two men were let into the bank's premises in London by a security supervisor. One man was a hacker, the other his overseer. While they failed to successfully carry out the plan, their goal was to install key logging software on the computers and then return to carry out fraudulent bank transfers (Lowe 2008). This plot involved a global network of conspirators, but according to former law enforcement agent, Phillip, an OCG in London and another group on the continent played a central role in carrying out the plot. They coordinated and recruited the various actors and oversaw the operation. Phillip did not want to name the groups as they were "ominous people" (UK-(F)LE-2).

Such involvement by OCGs, effectively as the recruiter/coordinator, was the connection between organised crime and cybercrime most commonly reported by former cybercriminals and hackers. In his later life as a security professional, Ahmed has been approached by a number of people seeking his services, which he regularly turns down. In one case a local drug dealer connected to a major syndicate was interested in hiring him to gather intelligence on specific individuals (most likely competitors) by hacking them (SEA-(F)CC-1). Casper, a Western European hacker, was convicted for his activities and later released. Not long afterwards, he was

approached by what he called “real criminals, very big criminals”. The criminals flew in to meet Casper and treated him very well in the hopes of wooing him to become involved in their criminal activities. This included a major jewelry heist in Europe, where he was to hack the alarm system of the target site. Casper politely declined the proposal (WE-(F)CC-2). Elsewhere in Western Europe, a similar story was recounted by former hacker Jeremy who was approached by a woman seeking his services for a job, but who he suspected may have been an undercover agent of one kind or another (W(E-(F)H-1).

These last two alternative roles are essentially two sides of the same coin. In both cases OCGs make use of their traditional skills on the money side and enforcing arrangements, but leave the technical elements of the job to others. Which category the activity fits into depends on whether those with technical skills approach the OCGs to assist with cashing out, or whether the organised crime groups look to bring in technical talent for their own scam. Sometimes it may be difficult to tell which is the case. Some of these connections between OCGs and cybercrime discussed above may tend towards a fifth category of organised crime involvement, but which may be outside the scope of cybercrime. In these cases, OCGs seek to recruit or partner with technical talent in order to enhance their existing operations, rather than engaging in cybercrime *per se*.

For instance, triads in Hong Kong have traditionally run prostitution but have found that new technologies can improve their efforts at marketing their service. They have built online websites that showcase the different prostitutes available and allow johns to book directly online (HK-(F)LE-2). Such websites are not unusual in the world of

modern prostitution, but in this case they are run by serious organised criminals and operated in a way to keep them safe from law enforcement, for instance, by keeping the servers in mainland China (HK-(F)LE-2). The triads are also active in online gambling, which essentially enhances their existing offline interests in the area. The casinos of Macao are known to be controlled by triad groups and play a key role in money laundering operations (Varese (forthcoming)). In Malaysia, the triads have found an intriguing way of providing gambling in a jurisdiction where it is illegal. Patrons enter a location where they can place bets on games such as roulette. But the casino itself is located elsewhere in the Philippines, with a video link up to the room in Malaysia showing the action. This geographical dispersion, along with the placement of servers overseas, complicates law enforcement attempts to curb the practice (MY-CSP-1). In the world of true online gambling where games are played on websites, there have also been suggestions of involvement by the Italian America mafia. This extends their traditional control of illicit gambling in the United States. In this case, these sites were also hosted offshore in jurisdictions like Costa Rica (see Menn 2010).

In a similar vein, there have been instances of drug traffickers employing technology to achieve their ends. There are murmurs of Mexican drug cartels kidnapping programmers to carry out tasks for them. Background information I gathered suggested that some of these might include hacking US agencies like Customs to gain intelligence and aid smuggling operations. Irfan, a Malaysian security professional, claimed that a friend of his had provided IT services to drug traffickers in the Golden Triangle in Southeast Asia (MY-CSP-4). Apparently even drug barons need Internet, email and adequate security. Perhaps the most famous interaction between drug

groups and technology was the hacking of Antwerp Port discovered in 2013. Drugs were hidden in containers that were moved through the port. It appears that a Netherlands based group hired hackers to compromise the port systems so that the relevant containers could be identified and then stolen before they were claimed for their true owner (Robertson and Riley 2015).

Sometimes it may be difficult to distinguish between this last category and the role that OCGs play in guiding certain cybercriminal schemes. Both involve the recruitment of technical actors by organised crime groups. The distinction essentially returns to the definition of cybercrime established in the introduction. If the use of the technology is playing a central role in the crime, such as making use of key loggers to facilitate a bank heist, it should be considered cybercrime. In cases where cyber is merely tangential to crime, such as the provision of IT services to drug traffickers in the Golden Triangle, it should not be considered cybercrime. But, of course, many of the examples fall between these two ends of the spectrum. Some might view certain examples discussed in category four as belonging in category five, and vice versa. Others might view acts, such as hacking to gain intelligence, as tangential to the core crime of trafficking drugs, but its own independent instance of cybercrime. Many of these questions become a matter of degree, which is not easily resolved and goes beyond the scope of this chapter. But the central point remains that the strict categorisation of what is and isn't cybercrime may not always be helpful in practice. Organised crime groups clearly do not draw such strict delineations in their own activities.

The point of this rather long digression is to say that OCGs are involved in cybercrime, but they do not necessarily have a large role in governing it. There are definitely examples of OCGs providing protection to cybercriminals. This may help with the overall ordering of the business, but it is not particularly widespread. When organised criminals are involved in cybercrime, it is much more likely that they are playing a role within the industry, rather than seeking to control it. Core roles are as investors, those who handle the money side of schemes, and acting as guiding hands in managing specific cybercrime operations. But even here it is important not to overstate matters and represent this as a complete takeover, as some have. While OCGs might be the first suspect when one thinks of offline cybercriminal governance, the evidence is not strong. Instead it is sensible to move onto the second suspect and the role that corrupt government agents are playing in protecting the cybercrime industry.

Corruption and Protection

This section focusses on the vital role that corrupt state officials and agents play within the cybercrime industry. As we saw above, there is only limited evidence that organised crime controls cybercrime on a large scale. Instead, it appears to be corrupt agents that provide the key governance function and help the cybercrime industry flourish in certain locations around the globe. The key idea in this section is that corrupt state agents act as protectors of cybercriminals. The main way in which they do this is to either fail to arrest the relevant criminals, tip them off about upcoming operations against them, or even intervene after the arrest has been made. The latter category might seem extreme but it is not without precedent. When Dmitry Golubov,

aka Script, was arrested in Ukraine in 2005, he was held in custody for six months before being released by a judge on the "advice" of two local politicians (Zetter 2007b).

While there were examples of OCGs providing protection to cybercriminals in my data, instances of state protection appeared far more regularly. Many of those who had not observed organised crime involvement in cybercrime were well aware of the law enforcement corruption that helps facilitate the phenomenon. This was the case in Russian cybercrime, where Vladimir and Aleks viewed the business as one largely of "geeks trading geeks" and where law enforcement protection was far more common than having the involvement of organised criminals (RUS-CSP-5, RUS-CSP-6). Former Ukrainian law enforcement agent Nikita believed that corruption was a major problem in relation to cybercrime flourishing in the country. For him, the central concern in the country was not about reforming the law, but enforcing it properly. In many instances, he believed that the law has not been enforced because of agents taking bribes (UKR-(F)LE-2).

While these instances may suggest corruption among low-level law enforcement agents, the problem may go much higher. Brian Krebs' investigation of Russian spam "businesses" suggests that large operations may seek protection from the highest levels of law enforcement and government. Drawing on databases of leaked communications and interviews, Krebs suggests that rival spammers Pavel Vrublevsky and Igor Gusev were funnelling money through Russian sports associations in order to purchase protection from the highly influential political and law enforcement figures who administer them (Krebs 2014, pp. 150-153). Aside from

this example, there are also a surprising number of cases that involve cybercriminals whose relatives are law enforcement officials or important political figures. The leading carder Roman Seleznev, who was arrested in the Maldives and extradited to the United States in 2014, is the son of a member of parliament in Russia (AP 2015). Flyman, who was placed in charge of the feared RBN is suggested to be the son of someone "who occupies a position of influence at a key Russian ministry" (Graham 2009, p. 173). On the law enforcement side, Alexander Rubatsky's father was a high-ranking police officer in Belarus (Krebs 2014, pp. 17-24). Meanwhile in *Fatal System Error*, Joseph Menn recounts an episode where UK agent Andy Crocker attempted to arrest a Russian cybercriminal based in Astrakhan. The suspect's father turned out to be the local police chief, leaving Crocker and his colleague holed up a hotel room in fear of their safety (Menn 2010, pp. 150-152).

Instances of corruption in the cybercrime area were rarely observed in the West by interview subjects, but participants often pointed to corruption elsewhere around the globe. Ex communist Romania appeared to have similar instances of protection as those found in the former Soviet Bloc states, such as payments to local law enforcement to prevent arrest (US-CSP-10). When in Romania, I learned that the (now former) police chief of Ramnicu Valcea, one of the geographical hubs of cyber fraud, had previously been arrested for tipping off criminal groups in the area about investigations and operations. Such arrests of officials may actually be a positive thing, highlighting the efforts of Romania to reduce corruption in the country, which was certainly noted by a number of interview participants (ROM-(F)LE-1, ROM-LE-1).

Corruption is also a major feature in relation to Nigerian cybercrime. While President Muhammadu Buhari was elected in 2015 on a platform to stamp out corruption, it has traditionally been a well-known challenge facing the country. Nigeria is regularly rated as one of the most corrupt countries in the world.[44] In this case, protection is somewhat "transactional" in relation to cybercrime. Rather than paying a regular protector as one might in Eastern Europe, some Nigerian cybercriminals simply pay a bribe to law enforcement agents to avoid an arrest or to be released subsequently (NIG-(F)LE-1). Yinka recalled being in a cyber café in the earlier days of Nigerian cybercrime, when most of the patrons were conducting illicit activities. The police raided the location and then demanded bribes to ensure release. In this case it was essentially a coordinated extortion attempt rather than a genuine investigation (NIG-CSP-4).

The Nigerian case suggests that the manner in which corruption interacts with cybercrime differs by context. Protection functions in particular ways, depending on the location in question. It is important to understand these local variations, but it is well beyond the scope of this chapter to engage in a country-by-country analysis. Nonetheless, the next subsection briefly addresses the system of corruption found in many former Soviet states. Given the significant contribution that those countries make to cybercrime, it is important to address this specific background in some detail. It helps to make better sense of how corruption supports the cybercrime industry in the region and how the specific system of protection functions.

[44] See, for instance, Transparency International's *Corruption Perceptions Index*, which is available at: http://www.transparency.org/cpi2015.

In order to understand how the cybercrime industry, corruption and protection interact, it is important to gain an understanding of how corruption functions within Eastern Europe. It is much more an ingrained aspect of the economy and political system, than it is a pure moral failing as some might see it. While many locals may resent it, or wish matters to be different, corruption is a part of daily life for most of the world's population (see Varese 2000). Perhaps counterintuitive for some, Fyodor wrote about his own view of corruption in this way:

> If fact, if you regard what you call "Russian corruption" as the factor, I'd say it is much beneficial for emerging businesses. It is very fertile grounds for unorthodox methods. They asking me a lot, whether it is bad, my answer, though that "chaos is not a disorder, it is just another type of order we do not understand". So it is with Russia, it have it's own ways, and they not always bad. You just have to learn how to operate in Russian environment, and soon you will learn that it is more pleasant that doing so in West. Although I don't advocate corruption, I regard it as inevitable, and, sometimes, lesser evil (EE-(F)CC-2).

For Fyodor the key element was to understand this Russian order, which accords theoretically with the concept of extra-legal governance (Dixit 2004). While key aspects of power and governance relate to formal political and legal institutions, there is a less formal system of conventions that also applies (Varese 2000). Some might disagree with Fyodor's analysis at particular points, but here I quote his views at length, and relatively unvarnished, to illustrate what might be an alien way of thinking for those in the West:

> Russia is very specific country, with very special order of things.

> It will be very hard to outline how the police works in Russia and it will take a lot to explain this. So, let's define, that in "Western" understanding, methods of operations of Russian police are corrupt. But this "corruption" is very questionable depending on the angle how you regard it. See, I very familiar with methods of works of Russian police, and generally they follow the orders of superiors and respect hierarchy, for example it will be very hard to believe that lieutenant investigating cybercrime will take bribe and sabotage case without knowledge of his superior. From this, it is evident that whole line of policing, "corrupt" as you call it, is well defined from high-above, they also follow the orders and rules, it is just so that those orders and rules are not in the book. So, it may be very good for you in Russia if you know "rules of the game", and follow it. And, knowing system, in both countries, I don't see how the American policing is less "corrupted" than Russian one, it is just that it is different kind of corruption. If in Russia it is bribe-taking and law-avoidance in favor of vague (let's call it) "game rules", in US it is bureaucracy, dictature, arrogance, embezzlement, and if we convert how much those "plagues" cost to system, I am sure that American ones will cost more to american taxpayers (EE-(F)CC-2).

Fyodor's account suggests that corruption in Eastern Europe is less the work of rogue agents, as it is institutionalised within the power structure. Many "illegal" actions also fall under the influence of different "legitimate" authorities. As a result, in order to make sense of many aspects of life in the former Soviet Bloc, it is vitally important to comprehend how the structures of authority function. Favarel-Garrigues (2011) provides a detailed history of policing of economic crimes in Russia, suggesting a degree of continuity between Soviet policing practices and those that followed. This includes instances of corruption and a degree of "tolerance" for economic crimes during the Soviet period, even though this contradicted official ideology. In this case and others, police have exhibited a degree of autonomy and might be viewed as "street level bureaucrats" (p. 3). But to fully comprehend the post Soviet system, the central concept of a protector must be understood. Varese outlines how this idea functions in the Russian context:

> In Russian slang, the word protection is *krysha* (lit. 'roof'). It was used during the Soviet period to refer to front activities for Committee of State Security (KGB), Military Intelligence (GRU), and Ministry of Internal Affairs (MVD) agents both in the country and abroad. Cultural institutions, publishing houses, embassies, and ministries all supplied a cover to people engaged in intelligence gathering. Since the Soviet Union collapsed, *krysha* refers to protection against ordinary criminals and 'unprofessional' racketeers, unruly business partners, and competitors. A *krysha* may ensure tax evasion and help in finding investment and credit opportunities. A Russian businessmen, in his testimony to a US Senate committee, maintains that to operate a successful business in Moscow one must 'pay the right government officials' and 'purchase a *krysha*,… which has come to mean protection. The more important you are, the higher the roof must be.' Reputable newspapers advise Russians to obtain a sound protection before starting any business. The search for a safe 'roof' is considered by *Komsomol'skaya Pravda* as the [sic] 'the most important element in the modern business world' (Varese 2001, p. 59).

In this context, protection may be provided by organised criminals, but it might just as easily be provided by state officials who are legally allowed to moonlight as private protectors (Varese 2001, pp. 59-61). As such their activity is not corrupt unless it sees their involvement in protecting illicit enterprises. Private protection may also be provided by security firms or by firms developing their own internal security arms (Varese 2001, pp. 61-68).

The system of protection works within a broader framework where aspects of criminal or corrupt behaviour have become somewhat normalised. Fyodor believed that this model of governance originated even before the Soviets, but that the tradition was enhanced under communism. He wrote his beliefs that one of the "few positive changes that communism inflicted on Soviet society is that feeling of social unity, relation, not so wrongly called "camaraderie". Though, origins of of such unity and

trust, I suppose, had nothing to do with communist theory, but rather with necessity to survive regime's oppression or to thrive and cheer at the times of hardships" (EE-(F)CC-2). In his view, those sent to prisons under the Soviets returned to society having adopted aspects of criminal culture. This counterculture then spread throughout society more generally, as it was useful to "thwart Soviet dictature and oppressions and survive in environment of suspicions, dictature and deprivations, some of those took roots too deeply among Soviet population" (EE-(F)CC-2). These traditions and growing cultural norms became an important aspect of life when the Soviet Union fell:

> Thus, post-Soviet society inherited this rich and controversial ruleset, and my generation were bought to it, as we learned about "camaraderie", help, mutual respect as well as distrust to authority from very young age; it is, naturally, was also very evident at the times when I grow up, that living and obeying by law will most likely not leads to prosperity or success, and it became even more evident, as capitalist values and goods, attractive and of high quality, flowed through "iron curtain" to the Soviet markets. It was very hard to prosper for a doctor or engineer, as those had miserable(though well respected) lives, and little or no salary, while crooks and swindlers prospered. This social difference became even more evident after Soviet Union collapse, and it was time when artful fraud, praised by such authors like Ilf and Petrov in their "12 chairs" and "Golden Calf", really became a form of art, well respected and loathed if successful. It is no wonder that new generation didn't want to be a doctors, they wanted to be crooks, and some wanted to be crooked doctors or engineers. Cybercriminals, in turn, is not much different, and learned very same rules of the game. However, they grew even more ruthless, since in real life criminal society and individuals, who you inevitably have to deal with if you choose life of fraud, will punish you for treason or disobedience, but cybercriminals were shield by the screen and keyboard from those, as well as they believed, from law and prosecution. For some, in late '90s cybercrime became form of ideal crime, undetected and unpunishable, while profitable and complex in it's nature (EE-(F)CC-2).

In practical terms, those high level positions in the state become very powerful figures. Their power is partly drawn from their official status. But they also derive great power from the unofficial status these positions bring:

> Thus, "corruption", in Russian interpretation, is none other than giving "due" to authority, not unlike paying taxes, or showing respect(read Nicholas Gogol's) to those in position of authority, as they were able to "get there" and you did not. In post-Soviet mind, paying bribes is not unlike paying taxes, and assisting you friends and your family to advance on social ladder in first place, it is very natural and unquestionable. So, to further this thinking, you can also note that in such mindset, it is not uncommon for one social layer to protect another in exchange for certain favors and benefits, each of those social layers could provide, not unlike old communist "camaraderie" (EE-(F)CC-2).

The cybercrime industry operates firmly within this system. A roof is of vital importance and it is common for cybercriminals in the former Soviet Bloc to have such a protector of one variety or another. This is part of doing business in the region. But for cybercriminals, their primary fear is arrest. Corrupt state officials can often greatly lessen such fears. This is fundamental to the success of the cybercrime industry in the region and the world. It provides the space for cybercriminals to build this illicit technology sector. It is the key factor that allows them to operate relatively openly and, as a result to build the large and sophisticated firms that were discussed in the previous chapter. The former Soviet Bloc is the technical engine of the global cybercrime industry. This system of patronage, corruption and protection is central to its overall success.

Conclusion

This chapter has argued that the protection of cybercriminals is central to the effective functioning of the industry. Just as in the online setting of cybercrime, a system of offline governance creates order that allows cybercriminals to operate more efficiently. In many criminal contexts, this role is performed by OCGs. The first section suggested that while there is some evidence for organised criminals protecting cybercriminals, it does not appear to be a widespread occurrence. Rather than seeking to govern cybercrime, OCGs are more likely to be involved *within* the industry, playing a specific role. But even this function is not as widespread as many would believe. Instead, the second section argued that true cybercriminal governance is commonly delivered by corrupt state officials and agents. Acting outside of their lawful authority, the central service that these agents provide is to protect cybercriminals from arrest, by tipping them off or subverting possible investigations. This is a vital service for cybercriminals because it allows them to operate in the relative open. Without strong requirements for secrecy, cybercriminals can collaborate with less fear, and the size of their enterprises grows accordingly. This protection afforded to cybercriminals offline helps explain much about the size of firms and the overall enhancement of the industry discussed in the last chapter.

Nonetheless, this manifestation of governance is curious in some ways. First, OCGs play a fairly limited role, even though they often seek to control a number of other criminal industries. It would not be a stretch for them to apply their skills to this new context, yet they do not in many instances. Second, the involvement of corrupt agents is often focussed on protection from arrest rather than arbitrating disputes between

cybercriminals, or driving competitors out of business. These are common forms of protection required by many criminals, alongside protection from arrest. But cybercriminals do not appear to require these services on a broad scale. It is beyond the scope of this chapter to address these issues in detail. But one could surmise that a lack of strong offline competition between cybercriminals might be a key factor in why these other governance services are not as popular as protection from arrest. When there are countless victims located across the world and any "turf" is virtual, disputes between cybercriminals in offline settings are unlikely. Such altercations are only likely to emerge when cybercriminals are operating in the same specific business, located physically in the same place and there is only a limited number of targets or customers available to them that they must fight over. Genuine competition may emerge in such cases. In these instances, protectors may find their other services in greater demand. But broadly speaking this does not appear to be the case across much of the cybercrime industry.

9. Conclusion

This thesis began with the story of Roman Seleznev. His tale is somewhat emblematic of the evolution of cybercrime in recent years. Gone are the days where cybercrime was built around hobby hacking and mischief. It is now a serious business. The big players look like illicit technology entrepreneurs, running their own firms with teams of programmers working for them. Other players might sell the product on marketplaces or perform various support functions. Those like Seleznev can bring in millions of dollars and live the high life. They can collaborate and trade with partners from around the globe. And they can threaten victims across the world. It has been the central argument of this thesis that a bona fide cybercrime industry has developed. In short, cybercrime has gone professional.

But this industrialisation is also puzzling: how can cybercriminals successfully cooperate on such a scale when their potential partners are anonymous criminals? It is challenging enough attempting to deal with criminals outside the protection of state institutions. But adding the layer of anonymity makes the instability of the situation even more extreme. One might expect cybercriminals to act alone or in small groups. But, as this thesis argues, the opposite is occurring. There has been widespread collaboration, the formation of large marketplaces, and the development of significant firms among other operational groupings. The second key focus of this thesis concerned this puzzle. It has attempted to undercover the mechanisms that have allowed this widespread cooperation and industrialisation to take place in a fundamentally distrustful world of anonymous criminals. As much as this is a study of

industry, it is also a study of anonymity: the obstacles it throws up and the ways it can be managed to achieve positive outcomes.

While this thesis is based on six years of fieldwork, its findings can only ever be suggestive. Part of this is due to the nature of qualitative data. But the bigger reason is that the world this study has sought to uncover, is simply too big for one scholar to investigate in considerable detail. 200 interviews is a significant number, but all of those connected to cybercrime number vastly more. All their perspectives cannot be included here. Instead, I have attempted to draw a map: to weave together many disparate elements into a whole and to better explain how exactly the cybercrime industry functions. Future studies will hopefully zero in on specific issues that have been identified. They will uncover new data and apply different research methods. In so doing, they may suggest nuances that have been missed, or even data that contradicts some of the findings here. At times, this felt like an endless project. And it is. But there reaches a point when insights must be shared so that the broader community can benefit and new research projects can emerge.

One of the challenges involved in carrying out this project was the retrospective nature of a number interviews. Many qualitative studies have a retrospective dimension to them. This can be beneficial as it may allow the participation of certain subjects, who might otherwise have been unable to contribute in their former roles or situations. It also allows the discussion of topics that may be sensitive in the present, but become less so over time. Of course, the passing of time may also fray memories. Meta-narratives could come into existence, informed by writings on various topics. Participants may partly "reconstruct" their memories based on this material. This is

particularly challenging when discussing historical events. For instance, the historical components of this thesis often draw on an oral history of cybercrime, which may be influenced by what has been written on the topic already. This was one reason I tried to limit my publication output while fieldwork was ongoing, so as not to taint the data with participants restating elements of what they read in preparation of meeting me. I also took pains to challenge certain narratives that appeared relatively neat, as well as bringing in other sources on these points to enhance triangulation. But, of course, complete accuracy can never be assured. Within a number of limitations, this thesis contributes as much as it can.

After a discussion of methods, the early chapters of this thesis examined the industrialisation of cybercrime. This began with an historical investigation of profit-driven cybercrime. Chapter 3 traced the evolution from the early days of hacking, which were largely built around intellectual curiosity, to the heavy focus on financially motivated activities that arrived later. This industrialisation also occurred organisationally, with the development of large online marketplaces like CarderPlanet and the subsequent operational groupings that followed. These groups directly carried out acts of cybercrime as teams, leaving behind the archetype of the lone wolf hacker. Drawing on this history, chapter 4 analysed the current state of cybercrime within a broad framework of industrial organisation. It noted the presence of key elements that one would expect to find in other illicit and licit industries: specialisation, professionalisation, markets, and firms.

The following chapters then moved to examine how this industrialisation could take place, given the challenges of anonymity. Chapter 5 addressed the question of identity

online and the way in which cybercriminal nicknames function as brands, making some form of cooperation possible in the first place. But ultimately, these brands are somewhat unstable, as nicknames can be quickly abandoned, with the central cost being the loss of accrued reputation. Cybercriminals face a key tension in this regard: the longer they maintain a nickname the more their reputation can develop, but maintaining a nickname for a long time means that cybercriminals are increasingly vulnerable to law enforcement investigations and tied to their past actions. There is no perfect solution to overcoming this tension and, instead, cybercriminals choose the strategy that best suits their needs, whether that means taking the risk of holding onto one handle, or varying handles regularly but trying to maintain a reputational trail of sorts with trusted partners.

Within the context of unstable identities and brands, chapter 6 examined what mechanisms cybercriminals employ to enhance cooperation. This discussion was built around trustworthiness and enforcement. In terms of trustworthiness, it was clear that reputation played a central role, but that appearance and performance were also important. In an online setting, monitoring and enforcement are challenging. Some forms of punishment are available, like DDoS and *doxing*, but these are far less threatening than physical violence. The development of institutions, particularly tied to forums, has made avenues of enforcement more effective and scalable to much larger numbers. For instance, the establishment of rules and the threat of exclusion, along with escrow services and arbitration appear particularly important. Overall, such forums seem to inject a level of governance into the underground economy and help grease the wheels of exchange. Of course, another key factor in this discussion is the large amounts of money that can be made through cybercrime, which may

outweigh some of the residual risks of collaborating with anonymous criminal partners.

Chapter 7 addressed an aspect of cybercrime that is often overlooked: the offline dimension. In some ways, this provides a very simple solution to the puzzle described above concerning how cybercriminals cooperate with anonymous partners. This chapter suggested that some cybercriminals simply sidestep this challenge by dealing with partners in the physical world instead of, or in addition to, those online. They might sacrifice their anonymity, or never seek to hide their identities from partners in the first place. Some might view this type of behaviour as puzzling in itself, but it goes to a central supposition that anonymity is not only a benefit in terms of protection from law enforcement interest, but is also costly in a number of ways. This chapter suggested that by forgoing anonymity, cybercriminals enhanced aspects of enforcement available to them. They could work with known partners locally and had a range of sanctions that they could employ, including the threat of violence. Without the concerns of dealing with anonymous partners, cooperation is improved. Firms were much more stable and could grow much larger, thereby buttressing the cybercrime industry as a whole.

Chapter 8 continued the discussion of the offline dimension and argued that the protection of cybercriminals is essential to the overall success of the industry. While OCGs play a number of roles in cybercrime, they are not taking over and governing the business on a wide scale. Instead, it is corrupt agents of the state that are primarily governing cybercrime in the physical world. As competition and disputes between cybercriminals are not a major concern, the chief function of these agents is to protect

cybercriminals from arrest. This allows cybercriminals in some countries to operate in a relatively open way. As a result, the sorts of large firms and enterprises identified in chapter 7, which begin to approximate licit technology companies, can flourish. Such corruption allows the cybercrime industry to reach the heights that it has.

It is hoped that these findings help to demystify cybercrime. There can be a tendency to view cybercrime as a magical new plane that is hidden and beyond comprehension. It can be seen as something so foreign that it challenges much of what we already know about crime and the world more broadly. In brutally honest terms, there does not appear much that is new about cybercrime. The definitions of cybercrime we use should probably reflect this. Certainly, there is little to justify the development of new theoretical frameworks around this case. Some details may differ, but the data in this thesis brought no substantial challenge to the existing theory I used, which has been widely applied to many other contexts. It may well be that other established frameworks from a range of disciplines are also applicable to cybercrime when applied to solid empirical findings.

The results of these chapters fit very well with the theoretical expectations outlined in the introduction. As noted in the literature, trustworthiness is an important component of cooperation. This was borne out in the case of online cybercrime, with reputation playing a particularly important role. But the other key theoretical plank, enforcement, was also present with common services like escrow and arbitration. The importance of institutions was clearly evident, particularly with regard to the development of online marketplaces. In keeping with the work of Douglass North and others, the evolution of cybercriminal institutions had precisely the effect that one would predict:

trade and collaboration flourished. Some level of governance was also apparent in this context, further enhancing cooperation and linking with theoretical expectations that some system of order may emerge in unexpected settings. The offline dimension of cybercrime also supported, rather than challenged, existing theory. Giving up anonymity served as a credible commitment for cooperation and opened up new (or rather old) avenues of enforcement, like the threat of physical violence. Offline cybercrime is also buttressed by a system of governance, in keeping with many other forms of crime.

The final point of this discussion is policy. What can be done about the cybercrime industry that is responsible for billions of losses and threatens victims across the world? Here I choose not to focus on law enforcement strategies and tactics. This is for a number of reasons. First, this has not been a focus of the study and other forms of data are probably better suited to this task. Second, as much as some subjects wanted to right past wrongs or establish a more trustworthy version of themselves going forward, the intention of the former cybercriminals who participated in this study was not to develop ways by which their old colleagues could be arrested or their operations disrupted. In fact, in one case, this position was specifically stated. Finally, as noted directly above, law enforcement action can only lead so far. Certain cybercriminals can be arrested and enterprises can be disrupted, but the scale of the threat remains immense. As one law enforcement agent put it to me, we "can't arrest our way out" of this situation (US-LE-3). Some attempt must be made to stem the flow of cybercriminals in the first instance.

The cybercrime industry is a tragedy. While some actors are simply career criminals who have found a new revenue source, across the world, numerous intelligent, capable and driven individuals are becoming involved in this enormous illicit enterprise. They spend considerable time innovating and refining their business. They make large amounts of money doing this. They are the heart of the business. But ultimately, all this effort is destructive rather than constructive. If this talent pool could be diverted away from cybercrime and into legitimate industry, there would be two positive developments. Not only would levels of cybercrime drop dramatically, but the efforts of these capable individuals would be turned to positive endeavours as well.

At the heart of the cybercrime industry is unemployment. When highly capable individuals can't find legitimate employment opportunities that challenge them and pay well, they turn elsewhere. It certainly helps that they often also operate in corrupt environments where such behaviour is more acceptable and law enforcement attention is limited. But ultimately cybercrime is work for them, whether they are simply looking for a steady job as a programmer or have the makings of an entrepreneur hoping to make millions. Without legitimate opportunities, they have created their own jobs. As this thesis has made clear, the scale of their work is impressive. Collectively, they have built an enormous profit-driven industry. It is a criminal Silicon Valley.

The great task of dramatically reducing cybercrime is to find ways to divert those who would become cybercriminals into legitimate employment. This could be achieved by widely recruiting technical talent out of regions where cybercrime is a particular

problem. Another method might be to invest heavily in the local technology sectors directly in those hotspots. This type of investment would provide the capital for entrepreneurs that is difficult to access locally, create more jobs and might have a positive effect on the broader economy. Such proposals are likely to succeed best in those places where offenders are more technical and opportunities in the technology sector might offer a direct exchange. The former Soviet Bloc might be a good place to focus on, given the outsize role that coders and programmers in that region play in cybercrime. Of course, in places like Romania or Nigeria, where offenders are smart but less directly connected to technical expertise, the challenge would be greater and more about the dynamics of the local economy and ways to improve overall employment prospects. The success of the technology sector in Romania demonstrates that increased technology jobs divert the more technical offenders out of the cybercrime business, but those focussed on lower level online fraud may still remain.

Of course, attempting to divert cybercriminals out of the criminal Silicon Valley and into legitimate employment faces some challenges. There are questions about whether those who are already steeped in the cybercrime business can be reformed or if they would make untrustworthy employees. Considerably more research is needed on such issues. A number of the former cybercriminals interviewed as part of this study, had either begun careers in legitimate industry or were wishing to do so. I certainly had faith, and hope, that a number would find success on their new path. If such past involvement in cybercrime turns out to be a risk factor, successful programs may have to target younger individuals and try and establish pathways towards the technology

sector before cybercrime becomes attractive. This is something that is already being experimented with in the West and could be applied more widely.

In terms of investing in local technology sectors, the main challenge is probably corruption. A core argument of this thesis has been that corruption facilitates cybercrime on a broad scale. As a result, one might be hesitant to inject large amounts of money into an economic system where the funds might be quickly misappropriated. One could also take steps to reduce overall corruption, but this is a intractable problem and moving well beyond the scope of this thesis. In basic terms, such an investment, and any other strategy to encourage potential cybercriminals to join the licit industry, should be encouraged. But considerably more research needs to be conducted in these areas to determine how successful programs could be implemented.

To sum up this point, and conclude this thesis, I end with a famous anecdote going back to the early days of profit-driven cybercrime (for varying accounts that are drawn on see Poulsen 2011, Cha 2003). On November 10, 2000, 20-year-old Alexey Ivanov was attending a job interview in Seattle. Ivanov was a talented programmer from Chelyabinsk in Russia, who had caught the attention of an American computer security start-up called Invita. The company was looking to expand their operations into Eastern Europe and believed that Ivanov, and his team of coders, was a perfect fit. Vasiliy Gorshkov accompanied Ivanov to the meeting, acting as his business manager of sorts. The meeting went well. Ivanov completed a hacking test that had been set up by the company and answered a series of questions. At one point, the CEO of Invita also asked Gorshkov about some recent computer intrusions in the

United States. He was curious if the two had been involved. He wanted to know how good they were.

After the interview was completed, the two Russians were driven away from the office towards their accommodation. But then the car stopped. The doors opened and FBI agents arrested both Ivanov and Gorshkov. It turned out that the two did know something about the recent computer intrusions the CEO had mentioned. Ivanov- aka subbsta – had been one of the leaders of a group called the Expert Group of Protection against Hackers. The *modus operandi* of this group was extortion: to hack into American Internet companies and steal credit card details or other data. They would then contact the company demanding payment not to release the data and, in return, would fix the holes that had allowed them access in the first place. If the companies didn't comply, they would then threaten to damage their systems. After this group hit a series of companies, the FBI began to uncover Ivanov's involvement.

Invita was not a real company. The office and its staff were not real either. They were all part of an elaborate sting to lure Ivanov into the country, after Russian authorities failed to take action. Unbeknownst to the two Russians, the office was filled with undercover FBI agents. The entire interview had been recorded with hidden cameras and microphones. The FBI had also installed key-logging software on the computers so that everything Ivanov typed was preserved. It was this way that an agent determined the password that allowed him access to a server in Russia and, controversially, to a trove of intelligence on the group's operations. From this, it was clear that the group's activities were coordinated, extensive and extremely lucrative. This evidence was suggestive of the enormous cybercrime industry that would soon

follow. But for those involved, even in the early days, it has always been about money and making a good living. Ivanov was a skilled coder. The sad irony is that he flew all the way to America because he wanted to work in the technology sector. He was willing to take the risk and shed his anonymity for it. He was not born to be a cybercriminal. He wanted a better life.

Bibliography

Primary Sources[*]

R v Kelly and Others, Southwark Crown Court, 2011, 35 [Case Summary].

R v Renu Subramanium and John McHugh, Blackfriars Crown Court, 2010 [Opening Note].

US v. Andrew Mantovani and Others, United States District Court, New Jersey, 2004 [indictment].

US v. Liberty Reserve S.A. and Others, United States District Court, Southern District of New York, 2013 [indictment].

US v. Morris, 928 F. 2d 504, United States Court of Appeals, 2nd Circuit 1991.

US v. Roman Seleznev and Others, United States District Court, Western District of Washington, 2011 [indictment].

US v. Roman Zolotarev and Others, United States District Court, Nevada, 2012 [indictment].

[*] Many other primary sources were consulted and informed the background to this project. But only those sources directly cited are listed here. I also do not list those cited documents which were furnished to me on the condition that they remain confidential.

Secondary Sources

Abreu, Dilip. 1988. "On the Theory of Infinitely Repeated Games with Discounting." *Econometrica* 56 (2):383-396.

Aguazue, Chima. 2013. *The Role of a Culture of Superstition in the Proliferation of Religio-Commercial Pastors in Nigeria*. Bloomington: Author House.

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. "Measuring the Cost of Cybercrime." In *The Economics of Information Security and Privacy*, edited by Rainer Böhme, 265-300. Berlin: Springer.

AP. 2015. "Russian MP Allegedly Plotted with Imprisoned Son to Escape US Custody." The Guardian, Last Modified October 8 2015, accessed September 14 2016. https://www.theguardian.com/world/2015/oct/08/russia-mp-valery-seleznev-plotted-son-escape-us-custody.

Axelrod, Robert. 2006. *The Evolution of Cooperation*. New York: Basic Books.

Baarda, Charlotte. 2015. "Human Trafficking for Sexual Exploitation from Nigeria into Western Europe: The Role of Voodoo Rituals in the Functioning of a Criminal Network." *European Journal of Criminology* 13 (2):1-17.

Babiak, Paul, and Robert Hare. *Snakes in Suits: When Psychopaths Go to Work*. New York: Regan Books.

Bailes, Kendall. 1978. *Technology and Society under Lenin and Stalin: Soviet Technical Intelligentsia, 1917-1941*. Princeton: Princeton University Press.

BBC. 2010. "Organiser of Darkmarket Fraud Website Jailed." BBC, Last Modified February 26 2010, accessed July 12 2016. http://news.bbc.co.uk/1/hi/uk/8539680.stm.

Belson, David. 2015. The State of the Internet (Q3). Akamai.

Bernard, H. Russell. 2011. *Research Methods in Anthropology*. Lanham: Altamira.

Bhattacharjee, Yudhijit. 2011. "Welcome to Hackerville: The Romanian Cybercriminal Hotspot." Wired, Last Modified February 7 2011, accessed January 12 2016. http://www.wired.co.uk/magazine/archive/2011/03/features/welcome-to-hackerville.

Black, Sharon, Brad Wilcox, and Brad Platt. 2014. "Nicknames in Prison: Meaning and Manipulation in Inmate Monikers." *Names* 62 (3):127-136.

Blau, John. 2004. "Russia - A Happy Haven for Hackers." ComputerWeekly.com, Last Modified May 2004, accessed September 14 2016. http://www.computerweekly.com/feature/Russia-a-happy-haven-for-hackers.

Bosworth, Mary, Debi Campbell, Bonita Demby, Seth Ferranti, and Michael Santos. 2005. "Doing Prison Research: Views From Inside." *Qualitative Inquiry* 11 (2):249-264.

Brannen, Julia. 1988. "The Study of Sensitive Subjects." *The Sociological Review* 36 (3):552-563.

Brenner, Susan. 2002. "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships." *North Carolina Journal of Law & Technology* 4 (1):1-50.

Brenner, Susan. 2010. *Cybercrime: Criminal Threats from Cyberspace*. Westport: Praeger.

Burgess, Robert. 1984. *In the Field: An Introduction to Field Research*. London: Allen & Unwin.
Campana, Paolo, and Federico Varese. 2013. "Cooperation in Criminal Organizations: Kinship and Violence as Credible Commitments." *Rationality and Society* 25 (3):263-289.
Carignan, Mira. 2015. "L'Origine Géographique en tant que Facteur Explicatif de la Cyberdélinquance " Masters, École de Criminologie, Université de Montréal.
Carter, Mike. 2015. "Accused Hacker Should Pay Defense Cost, Prosecutors Say." The Seattle Times, Last Modified March 20 2015, accessed September 7 2016. http://www.seattletimes.com/seattle-news/crime/accused-hacker-should-pay-defense-cost-prosecutors-say/.
Center for Strategic and International Studies. 2014. Net Losses: Estimating the Global Cost of Cybercrime. McAfee.
Cha, Ariana. 2003. "A Tempting Offer for Russian Pair." The Washington Post, Last Modified May 19 2003, accessed September 15 2016. https://www.washingtonpost.com/archive/politics/2003/05/19/a-tempting-offer-for-russian-pair/2c6a5407-8378-4939-8491-038efab2c5fb/.
Church, Jeffrey, and Roger Ware. 2000. *Industrial Organisation: A Strategic Approach*. Boston: Irwin McGraw-Hill.
Coase, Ronald. 1937. "The Nature of the Firm." *Economica* 4 (16):386-405.
Coase, Ronald. 1988. *The Firm, the Market and the Law*. Chicago and London: The University of Chicago Press.
Cohen, Lawrence, and Marcus Felson. 1979. "Social Change and Crime Rates: A Routine Activity Approach." *American Sociological Review* 44 (4): 588-608.
Cohen, Lawrence, and Kenneth Land. 1987. "Age Structure and Crime: Symmetry Versus Asymmetry and the Projection of Crime Rates Through the 1990s." *American Sociological Review* 52 (2).
Coleman, James. 1988. "Social Capital in the Creation of Human Capital." *American Journal of Sociology* 94 (Supplement: Organizations and Institutions):95-120.
Coleman, James. 1990. *Foundations of Social Theory*. Cambridge, Mass and London: Belknap Press of Harvard University Press.
Cook, Karen, Russell Hardin, and Margaret Levi. 2005. *Cooperation Without Trust?* New York: Russell Sage Foundation.
Cook, Karen, Chris Snijders, Vincent Buskens, and Coye Cheshire, eds. 2009. *eTrust: Forming Relationships in the Online World*. New York: Russell Sage Foundation.
Dasgupta, Partha. 1988. "Trust as a Commodity." In *Trust: Making and Breaking Cooperative Relations*, edited by Diego Gambetta, 49-72. Oxford: Basil Blackwell.
Davies, Caroline. 2010. "Welcome to DarkMarket – Global One-Stop Shop for Cybercrime and Banking Fraud." The Guardian, Last Modified January 14 2010, accessed August 1 2011. http://www.guardian.co.uk/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley.
Décary-Hétu, David, and Benoit Dupont. 2012. "The Social Network of Hackers." *Global Crime* 13 (3):160-175.
Décary-Hétu, David, and Benoit Dupont. 2013. "Reputation in a Dark Network of Online Criminals." *Global Crime* 14 (2-3):175-196.

Décary-Hétu, David, and Anna Leppänen. 2016. "Criminals and Signals: An Assessment of Criminal Performance in the Carding Underworld." *Security Journal* 29 (3):442-460.
Dellarocas, Chrysanthos. 2003. "The Digitization of Word-of-Mouth: Promise and Challenges of Online Feedback Mechanisms." *Management Science* 49 (10):1407-1424.
Densley, James. 2013. *How Gangs Work: An Ethnography of Youth Violence*. New York: Palgrave Macmillan.
Denzin, Norman. 1978. *The Research Act: A Theoretical Introduction to Sociological Methods*. New York: McGraw-Hill.
Diekmann, Andreas, Ben Jann, and David Wyder. 2009. "Trust and Reputation in Internet Auctions." In *eTrust: Forming Relationships in the Online World*, edited by Karen Cook, Chris Snijders, Vincent Buskens and Coye Cheshire, 139-165. New York: Russell Sage Foundation.
Dixit, Avinash. 2004. *Lawlessness and Economics: Alternative Modes of Governance*. Princeton and Oxford: Princeton University Press.
Dreyfus, Suelette, and Julian Assange. 2012. *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Edinburgh: Canongate.
Dupont, Benoit. 2014. "Skills and Trust: A Tour Inside the Hard Drives of Computer Hackers." In *Crime and Networks*, edited by Carlo Morselli, 195-217. New York: Routledge.
Dupont, Benoît, Anne-Marie Côté, Claire Savine, and David Décary-Hétu. 2016. "The Ecology of Trust among Hackers." *Global Crime* 17 (129-151).
Durkheim, Emile. *The Division of Labour in Society*. Basingstoke: Palgrave Macmillan.
Favarel-Garrigues, Gilles. *Policing Economic Crime in Russia: From Soviet Planned Economy to Privatisation*. London: C Hurst.
FBI. 2014. "A Byte Out of History: $10 Million Hack, 1994-Style." Federal Bureau of Investigation, Last Modified January 31 2014, accessed August 31 2015. https://www.fbi.gov/news/stories/2014/january/byte-out-of-history-10-million-hack-1994-style.
Fehr, Ernst, and Herbert Gintis. 2007. "Human Motivation and Social Cooperation: Experimental and Analytical Foundations." *Annual Review of Sociology* 33:43-64.
Franklin, Jason, Adrian Perrig, Vern Paxson, and Stefan Savage. 2007. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants." Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07), Alexandria, October 29 - November 02.
Furnell, Steven. 2002. *Cybercrime: Vandalizing the Information Society*. Boston; London: Addison-Wesley.
Gambetta, Diego. 1993. *The Sicilian Mafia: The Business of Private Protection*. Cambridge and London: Harvard University Press.
Gambetta, Diego. 2009a. *Codes of the Underworld: How Criminals Communicate*. Princeton and Oxford: Princeton University Press.
Gambetta, Diego. 2009b. "Signaling." In *The Oxford Handbook of Analytical Sociology*, edited by Peter Bearman and Peter Hedstrom, 168-194. Oxford: Oxford University Press.
Genders, Elaine, and Elaine Player. 1995. *Grendon: A Study of a Therapeutic Prison*. Oxford: Clarendon Press.

Giallombardo, Rose. 1966. "Interviewing in the Prison Community." *The Journal of Criminal Law, Criminology, and Police Science* 57 (3):318-324.
Gibbons, Robert. 2001. "Trust in Social Structures: Hobbes and Coase Meet Repeated Games." In *Trust in Society*, edited by Karen Cook. New York: Russell Sage Foundation.
Glenny, Misha. 2011. *DarkMarket: CyberThieves, CyberCops and You*. London: Bodley Head.
Goffman, Alice. 2014. *On the Run: Fugitive Life in an American City*. Chicago: The University of Chicago Press.
Goldman, David. 2011. "The Cyber Mafia has Already Hacked You." CNN Money, Last Modified July 27 2011, accessed September 14 2016. http://money.cnn.com/2011/07/27/technology/organized_cybercrime/.
Grabosky, Peter. 2001. "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10 (2):243-249.
Graham, James, ed. 2009. *Cyber Fraud: Tactics, Techniques, and Procedures*. Boca Raton: CRC Press.
Graham, Loren. 1993. *Science in Russia and the Soviet Union: A Short History*. Cambridge: Cambridge University Press.
Graham, Loren. 1998. *What Have We Learned about Science and Technology from the Russian Experience?* Stanford: Stanford University Press.
Granovetter, Mark. 1985. "Economic Action and Social Structure: The Problem of Embeddedness." *American Journal of Sociology* 91 (3):481-510.
Gravelle, Hugh, and Ray Rees. 2004. *Microeconomics*. Harlow: Prentice Hall.
Greif, Avner. 1989. "Reputation and Coalitions in Medieval Trade: Evidence on the Maghribi Traders." *Journal of Economic History* 49 (4):857-882.
Grow, Brian, and Jason Bush. 2005. "Hacker Hunters." Bloomberg, Last Modified May 30 2005, accessed July 12 2016. http://www.bloomberg.com/news/articles/2005-05-29/hacker-hunters.
Hafner, Katie, and Matthew Lyon. 2006. *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Simon & Schuster.
Halpern, Jake. 2015. "Bank of the Underworld." The Atlantic, Last Modified May 2015, accessed September 13 2016. http://www.theatlantic.com/magazine/archive/2015/05/bank-of-the-underworld/389555/.
Hardin, Russell. 2001. "Conceptions and Explanations of Trust." In *Trust in Society*, edited by Karen Cook, 3-39. New York: Russell Sage Foundation.
Hay, Donald, and Drek Morris. 1979. *Industrial Economics: Theory and Evidence*. Oxford: Oxford University Press.
Hayek, Friedrich. 1988. *The Fatal Conceit*. London: Routledge.
Hayek, Friedrich. 2006. *The Constitution of Liberty*. London: Routledge.
Henderson, Scott. 2007. *The Dark Visitor*: Self Published.
Hirschi, Travis, and Michael Gottfredson. 1983. "Age and the Explanation of Crime." *The American Journal of Sociology* 89 (3):552-584.
Hobbes, Thomas. 2012 [1651]. *Leviathan*. Oxford: Oxford University Press.
Holt, Thomas. 2013a. "Examining the Forces Shaping Cybercrime Markets Online." *Social Science Computer Review* 31 (2):165-177.
Holt, Thomas. 2013b. "Exploring the Social Organisation and Structure of Stolen Data Markets." *Global Crime* 14 (2-3):155-174.
Holt, Thomas, and Adam Bossler. 2014. "An Assessment of the Current State of Cybercrime Scholarship." *Deviant Behaviour* 35 (1):20-40.

Holt, Thomas, and Eric Lampke. 2010. "Exploring Stolen Data Markets Online: Products and Market Forces." *Criminal Justice Studies* 23 (1):33-50.
Holt, Thomas, Olga Smirnova, Yi Ting Chua, and Heith Copes. 2015. "Examining the Risk Reduction Strategies of Actors in Online Criminal Markets." *Global Crime* 16 (2):81-103.
Hong, Nicole. 2016. "More Street Gangs Turn to Financial Crimes." The Wall Street Journal, Last Modified March 7 2016, accessed September 14 2016. http://www.wsj.com/articles/more-street-gangs-turn-to-financial-crimes-1457379074.
Honigmann, J.J. 1982. "Sampling in Ethnographic Fieldwork." In *Field Research: A Source Book and Field Manual*, edited by Robert Burgess. London: Allen & Unwin.
Hoyle, Rick, Monica Harris, and Charles Judd. 2002. *Research Methods in Social Relations*. Fort Worth: Wadsworth.
Hutchings, Alice. 2013. "Hacking and Fraud: Qualitative Analysis of Online Offending and Victimization." In *Global Criminology: Crime and Victimization in a Globalized Era*, edited by K Jaishankar and Natti Ronel. Boca Raton: CRC Press.
Hutchings, Alice, and Thomas Holt. 2015. "A Crime Script Analysis of the Online Stolen Data Market." *British Journal of Criminology* 55 (3):596-614.
Israel, Mark, and Iain Hay. 2006. *Research Ethics for Social Scientists*. Thousand Oaks: Sage.
Jacobs, Bruce. 2006. "The Case for Dangerous Fieldwork." In *The Sage Handbook of Fieldwork*, edited by Dick Hobbs and Richard Wright, 157-168. Thousand Oaks: Sage.
Johnson, Terence. 2016. *Professions and Power*. London: Routledge.
Jordan, Tim, and Paul Taylor. 1998. "A Sociology of Hackers." *The Sociological Review* 46 (4):757-780.
Katz, Jack. 1988. *Seductions of Crime: Moral and Sensual Attractions in Doing Evil*. New York: Basic Books.
King, Gary, Robert Keohane, and Sidney Verba. 1994. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton: Princeton University Press.
King, Roy. 2000. "Doing Research in Prisons." In *Doing Research on Crime and Justice*, edited by Roy King and Emma Wincup, 285-312. Oxford: Oxford University Press.
Klein, Benjamin, and Keith Leffler. 1981. "The Role of Market Forces in Assuring Contractual Performance." *Journal of Political Economy* 89 (4):615-641.
Krebs, Brian. 2007. "Shadowy Russian Firm Seen as Conduit for Cybercrime." The Washington Post, Last Modified October 13 2007, accessed September 25 2015. http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html.
Krebs, Brian. 2008. "Ukrainian CyberCrime Boss Leads Political Party." The Washington Post, Last Modified March 13 2008, accessed September 17 2015. http://voices.washingtonpost.com/securityfix/2008/03/ukranian_cybercrime_boss_leads.html.
Krebs, Brian. 2013. "The World Has No Room For Cowards." KrebsonSecurity, Last Modified March 15 2013, accessed September 22 2015. http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/.

Krebs, Brian. 2014. *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door*. Naperville: Sourcebooks.
Krebs, Brian. 2015. "The Darkode Cybercrime Forum, Up Close." KrebsonSecurity, Last Modified July 15 2015, accessed September 18 2015. http://krebsonsecurity.com/2015/07/the-darkode-cybercrime-forum-up-close/.
Kshetri, Nir. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Berlin: Springer.
Kvale, Steinar. 1996. *InterViews: An Introduction to Qualitative Research Interviewing*. Thousand Oaks: Sage.
Lawrence, Dune. 2015. "An Identity Thief Explains the Art of Emptying Your Bank Account." Bloomberg Businessweek, Last Modified July 15 2015, accessed September 23 2015. http://www.bloomberg.com/news/articles/2015-07-15/an-identity-thief-explains-the-art-of-emptying-your-bank-account.
Legard, Robin, Jill Keegan, and Kit Ward. 2003. "In-Depth Interviews." In *Qualitative Research Practice*, edited by Jane Ritchie and Jane Lewis, 138-169. Thousand Oaks: Sage.
Levi, Michael. 2008. *The Phantom Capitalists: The Organisation and Control of Long-Firm Fraud*. Aldershot: Ashgate.
Levy, Steven. 2010. *Hackers: Heroes of the Computer Revolution*. Sebastopol, CA: O'Reilly Media.
Liebling, Alison. 1999. "Doing Prison Research: Breaking the Silence." *Theoretical Criminology* 3 (2):147-173.
Littman, Jonathan. 1993. "The Last Hacker: He Called Himself Dark Dante. His Compulsion Led Him to Secret Files and, Eventually, the Bar of Justice." Los Angeles Times, Last Modified September 12 1993, accessed August 31 2015. http://articles.latimes.com/1993-09-12/magazine/tm-34163_1_kevin-poulsen.
Littman, Jonathan. 1997. *The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen*. New York: Little, Brown and Company.
Lowe, Felix. 2008. "Sumitomo Mitsui: The Bank that Thwarted the £220 Million Heist." The Telegraph, Last Modified June 25 2008, accessed September 14 2016. http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/2792188/Sumitomo-Mitsui-The-bank-that-thwarted-the-220-million-heist.html.
Lusthaus, Jonathan. 2012. "Trust in the World of Cybercrime." *Global Crime* 13 (2):71-94.
Lusthaus, Jonathan. 2013a. Call Me i$Hm@eL. Pacific Standard (Nov/Dec).
Lusthaus, Jonathan. 2013b. "How Organised is Organised Cybercrime?" *Global Crime* 14 (1):52-60.
Lusthaus, Jonathan. 2014. "Electronic Ghosts." *Democracy* Winter (31).
Maher, Lisa. 1997. *Sexed Work: Gender, Race, and Resistance in a Brooklyn Drug Market*. Oxford: Clarendon Press.
Marshall, Catherine, and Gretchen Rossman. 1999. *Designing Qualitative Research*. Thousand Oaks: Sage.
Matfin, Carol. 2011. "Doing Research in a Prison Setting." In *Doing Criminological Research*, edited by Victor Jupp, Pamela Davies and Peter Francis, 215-234. Los Angeles and London: SAGE.
Maurer, David, and Allan Futrell. 1982. "Criminal Monickers." *American Speech* 57 (4):243-255.
Maxwell, Joseph. 1996. *Qualitative Research Design*. Thousand Oaks: Sage.

McCarthy, Bill, John Hagan, and Lawrence E. Cohen. 1998. "Uncertainty, Cooperation, and Crime: Understanding the Decision to Co-Offend." *Social Forces* 77 (1):155-184.
McCracken, Grant. 1988. *The Long Interview*. Newbury Park: Sage.
McCusker, Rob. 2006. "Transnational Organised Cyber Crime: Distinguishing Threat from Reality." *Crime, Law and Social Change* 46 (4-5):257-273.
McQuade, Samuel. 2006. *Understanding and Managing Cybercrime*. Boston: Allyn and Bacon.
Mell, Andrew. 2012. Reputation in the Market for Stolen Data. In *Department of Economics Discussion Paper Series*. Oxford: University of Oxford.
Menn, Joseph. 2010. *Fatal System Error*. New York: PublicAffairs.
Milgrom, Paul, Douglass North, and Barry Weingast. 1990. "The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs." *Economics and Politics* 2 (1):1-23.
Mills, Elinor. 2009. "Q&A: FBI Agent Looks Back on Time Posing as a Cybercriminal." CNET News, Last Modified August 15 2009, accessed August 17 2011. http://news.cnet.com/8301-1009_3-10234872-83.html.
Mitnick, Kevin D., and William L. Simon. 2011. *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. New York; London: Little, Brown and Company.
Morgan, Steve. 2016. "Cyber Crime Costs Projected To Reach $2 Trillion by 2019." Forbes, Last Modified January 17 2016, accessed September 7 2016. http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/ - 73c2fe6d3bb0.
Morris, Terence, Pauline Morris, and Barbara Barer. 1963. *Pentonville: A Sociological Study of an English Prison*. London: Routledge.
Motoyama, Marti, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey Voelker. 2011. "An Analysis of Underground Forums." Internet Measurement Conference 2011, Berlin, November 2.
Murphy, Alexandra and Sudhir Venkatesh. 2006. "Vice Careers: The Changing Contours of Sex Work in New York City." *Qualitative Sociology* 29 (2): 129-154.
Newman, Donald. 1958. "Research Interviewing in Prison." *The Journal of Criminal Law, Criminology, and Police Science* 49 (2):127-132.
Nightingale, John. 1978. "On the Definition of `Industry' and `Market'." *The Journal of Industrial Economics* 27 (1):31-40.
North, Douglass. 1991. "Institutions." *The Journal of Economic Perspectives* 5 (1):97-112.
Nozick, Robert. 1974. *Anarchy, State and Utopia*. Oxford: Blackwell.
O'Neill, Sean. 2001. "Girl, 8, Raped to Order on the Internet." The Telegraph, Last Modified February 14 2001, accessed September 20 2016. http://www.telegraph.co.uk/news/uknews/1322551/Girl-8-raped-to-order-on-the-internet.html.
Olson, Mancur. 1971. *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge: Harvard University Press.
Ostrom, Elinor. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge: Cambridge University Press.
Paoli, Letizia, Victoria Greenfield, and Peter Reuter. 2009. *The World Heroin Market: Can Supply Be Cut?* Oxford: Oxford University Press.

Parker, Stanley. 1981. *The Sociology of Industry*. London and Boston: Allen and Unwin.
Patton, Michael. 2002. *Qualitative Research and Evaluation Methods*. Thousand Oaks: Sage.
Pileggi, Nicholas. 1986. *Wiseguy: Life in a Mafia Family*. New York: Pocket Books, Simon & Schuster.
Pistone, Joseph. 1987. *Donnie Brasco: My Undercover Life in the Mafia*. London: Hodder.
Poulsen, Kevin. 2011. *Kingpin*. New York: Crown Publishers.
Pulkkinen, Levi. 2015. "Piles of Cash, Bunches of Bling and a Public Defender?". Seattle Post-Intelligencer, Last Modified January 16 2015, accessed September 7 2016. http://www.seattlepi.com/local/article/Piles-of-cash-bunches-of-bling-and-a-public-6021422.php.
Ragan, Steve. 2012. "Eight Arrested in Moscow After Allegedly Stealing Millions Using Carberp Trojan." Security Week, Last Modified March 21 2012, accessed September 25 2015. http://www.securityweek.com/eight-arrested-moscow-after-allegedly-stealing-millions-using-carberp-trojan.
Resnick, Paul, and Rihard Zeckhauser. 2002. "Trust among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System." In *The Economics of the Internet and E-Commerce*, edited by Michael Baye, 127-157. Amsterdam: Elsevier Science.
Reuter, Peter. 1983. *Disorganized Crime: The Economics of the Visible Hand*. Cambridge, Mass; London: MIT Press.
Ritchie, Jane, Jane Lewis, and Gillian Elam. 2003. "Designing and Selecting Samples." In *Qualitative Research Practice*, edited by Jane Ritchie and Jane Lewis, 77-108. Thousand Oaks: Sage.
Robertson, Jordan, and Michael Riley. 2015. "The Mob's IT Department." Bloomberg, Last Modified July 7 2015, accessed September 14 2016. http://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/.
RT. 2014. "Russian MP's Son to Remain in Custody in Seattle Until Hacking Trial." Russia Today, Last Modified August 16 2014, accessed September 7 2016. https://www.rt.com/news/180752-seleznyov-seattle-custody-trial/.
Rubin, Herbert, and Irene Rubin. 1995. *Qualitative Interviewing: The Art of Hearing Data*. Thousand Oaks: Sage.
Sanchez-Jankowski, Martin. 1991. *Islands in the Street*. Berkley and Oxford: University of California Press.
Schelling, Thomas. 1971. "What is the Business of Organized Crime." *Journal of Public Law* 20 (1):71-84.
Schelling, Thomas. 1980. *The Strategy of Conflict*. Cambridge: Harvard University Press.
Schelling, Thomas. 2006. *Strategies of Commitment*. Camrbidge, Massachusetts: Harvard University Press.
Shortland, Anja, and Federico Varese. 2014. "The Protector's Choice." *The British Journal of Criminology* 54 (5):741-764.
Singel, Ryan. 2008. "Turkish Police Arrest Alleged ATM Hacker-Kidnapper." Wired, Last Modified September 12 2008, accessed September 13 2016. https://www.wired.com/2008/09/turkish-police/.
Skarbek, David. 2011. "Governance and Prison Gangs." *American Political Science Review* 105 (4):702-716.

Slatalla, Michelle, and Joshua Quittner. 1995. *Masters of Deception: The Gang that Ruled Cyberspace*. London: Vintage.
Smith, Adam. 1999 [1776]. *The Wealth of Nations*. London: Penguin.
Sorensen, Robert. 1950. "Interviewing Prison Inmates." *Journal of Criminal Law and Criminology* 41 (2):180-182.
Spence, Michael. 1973. "Job Market Signaling." *Quarterly Journal of Economics* 87 (3):355-374.
Stoll, Cliff 2007. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Pocket Books.
Sullivan, Arthur, and Steven Sheffrin. 2003. *Economics: Principles in Action*. Upper Saddle River: Pearson Prentice Hall.
Sykes, Gresham. 1958. *The Society of Captives: A Study of a Maximum Security Prison*. Princeton: Princeton University Press.
Sztompka, Piotr. 1999. *Trust: A Sociological Theory*. Cambridge: Cambridge University Press.
Tade, Oludayo. 2013. "A Spiritual Dimension to Cybercrime in Nigeria: The 'Yahoo Plus' Phenomenon." *Human Affairs* 23 (4):689–705.
The New York Times. 1997. "Theft of Credit Card Numbers From Internet Leads to Arrest." The New York Times, Last Modified May 23 1997, accessed August 31 2015. http://www.nytimes.com/1997/05/23/us/theft-of-credit-card-numbers-from-internet-leads-to-arrest.html.
The Telegraph. 2009. "Gary McKinnon Profile: Autistic 'Hacker' Who Started Writing Computer Programs at 14." The Telegraph, Last Modified January 23 2009, accessed September 7 2016. http://www.telegraph.co.uk/news/worldnews/northamerica/usa/4320901/Gary-McKinnon-profile-Autistic-hacker-who-started-writing-computer-programs-at-14.html.
Timperley, Stuart, and Michael Osbaldeston. 1975. "The Professionalization Process: A Study of an Aspiring Occupational Organization." *The Sociological Review* 23 (3):607-627.
UNODC. 2013. Comprehensive Study on Cybercrime. Vienna: United Nations.
USDOJ. 2005. "Six Defendants Plead Guilty in Internet Identity Theft and Credit Card Fraud Conspiracy." The United States Department of Justice, Last Modified November 18 2005, accessed July 12 2016. https://www.justice.gov/archive/opa/pr/2005/November/05_crm_619.html.
USDOJ. 2013. "Ukrainian National Who Co-founded Cybercrime Marketplace Sentenced to 18 Years in Prison." The United States Department of Justice, Last Modified December 12 2013, accessed September 17 2015. http://www.justice.gov/opa/pr/ukrainian-national-who-co-founded-cybercrime-marketplace-sentenced-18-years-prison.
Varese, Federico. 2000. "Pervasive Corruption." In *Economic Crime in Russia*, edited by Alena Ledeneva and Marina Kurkchiyan, 99-111. The Hague: Kluwer Law International.
Varese, Federico. 2001. *The Russian Mafia: Private Protection in a New Market Economy*. Oxford: Oxford University Press.
Varese, Federico. 2010. "What is Organized Crime?" In *Organized Crime: Critical Concepts in Criminology*, edited by Federico Varese, 1-33. New York: Routledge.
Varese, Federico. 2011. *Mafias on the Move*. Princeton and Oxford: Princeton University Press.

Varese, Federico. (forthcoming). *Mafia Life*. London: Profile.
Verini, James. 2010. "The Great Cyberheist." The New York Times, Last Modified November 10 2010, accessed September 3 2015. http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?_r=1.
Wall, David. 1998. "Catching Cybercriminals: Policing the Internet." *International Review of Law, Computers & Technology* 12 (2):201-218.
Wall, David, ed. 2001a. *Crime and the Internet*. London: Routledge.
Wall, David. 2001b. "Cybercrimes and the Internet." In *Crime and the Internet*, edited by David Wall, 1-17. London: Routledge.
Wall, David. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity.
Wall, David. 2008. "What are Cybercrimes?" *Criminal Justice Matters* 58 (1):20-21.
Wall, David. 2014. "Internet Mafias? The Dis-Organisation of Crime on the Internet." In *Organized Crime, Corruption and Crime Prevention*, edited by Stefano Caneppele and Francesco Calderoni, 227-238. Cham: Springer.
Whyte, William Foote. 1943. *Street Corner Society*. Chicago: University of Chicago Press.
Wilber, Del Quentin, and Chris Strohm. 2015. "Accused Russian Hacker on Tropical Holiday Nabbed by U.S. Agents." Bloomberg, Last Modified March 11 2015, accessed September 7 2016. http://www.bloomberg.com/news/articles/2015-03-11/accused-russian-hacker-on-tropical-holiday-nabbed-by-u-s-agents.
Wilson, Craig. 1997. "What's in a Name? Gang Monikers." FBI Law Enforcement Bulletin, accessed July 19 2016. https://www2.fbi.gov/publications/leb/1997/may972.htm.
Xakep.ru. 2002. Interview with a Carder. Xakep.ru.
Yar, Majid. 2005. "The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory." *European Journal of Criminology* 2 (4):407-427.
Yar, Majid. 2013. *Cybercrime and Society*. London; Thousand Oaks: SAGE Publications.
Yip, Michael, Craig Webber, and Nigel Shadbolt. 2013. "Trust Among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing." *Policing and Society* 23 (4):516-539.
Zahavi, Amotz. 1975. "Mate Selection: A Selection for a Handicap." *Journal of Theoretical Biology* 53 (1):205-214.
Zaitzow, Barbara. 1998. "Nickname Usage by Gang Members." *Journal of Gang Research* 5 (3):29-40.
Zetter, Kim. 2007a. "I Was a Cybercrook for the FBI." Wired, Last Modified January 30 2007, accessed September 12 2016. http://archive.wired.com/politics/onlinerights/news/2007/01/72515?currentPage=all.
Zetter, Kim. 2007b. "Tracking the Russian Scammers." Wired, Last Modified January 31 2007, accessed September 17 2015. http://archive.wired.com/politics/onlinerights/news/2007/01/72605.
Zetter, Kim. 2010. "Ukrainian Carding King 'Maksik' Was Lured to Arrest." Wired, Last Modified July 28 2010, accessed September 12 2016. https://www.wired.com/2010/07/maksik-lured-to-arrest/.
Zhang, Sheldon. 2008. *Chinese Human Smuggling Organizations: Families, Social Networks, and Cultural Imperatives*. Stanford: Stanford University Press.

Appendix: List of Participants

Australia (AUS)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Lachlan	Australian Cybersecurity Professional 1	2013	In Person/47.4	AUS-CSP-1
2	Liam	Former Australian Law Enforcement Agent 1	2013	In Person/39.13	AUS-(F)LE-1
3,4	Max, Harrison	Australian Law Enforcement Agent 1, Australian Law Enforcement Agent 2	2013	In Person/ Unrecorded Interview	AUS-LE-1; AUS-LE-2
5,6	Mia, Amelia	Australian Law Enforcement Agent 3, Australian Law Enforcement Agent 4	2013	In Person/Informal Discussion	AUS-LE-3; AUS-LE-4
7	Isaac	Australian Cybersecurity Professional 2	2013	In Person/48.09	AUS-CSP-2
8	Mitchell	Australian Cybersecurity Professional 3	2013	Phone/27.51	AUS-CSP-3

Brazil (BRA)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Antonio	Former Brazilian Law Enforcement Agent 1	2014	In Person/29.11	BRA-(F)LE-1
2	Rodrigo	Brazilian Cybersecurity Professional 1	2014	In Person/44.47	BRA-CSP-1

China (CHN)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Neil	Expatriate Cybersecurity Professional based in China 1	2014	In Person/41.49	CHN(E)-CSP-1
2	Charles	Former Expatriate Cybersecurity Professional based in China 1	2014	In Person/Informal Discussion	CHN(E)-(F)CSP-1
3	Zhou	Chinese Cybersecurity Professional 1	2014	In Person/49.38	CHN-CSP-1

4	Tony	Chinese Cybersecurity Professional 2	2014	In Person/Informal Discussion	CHN-CSP-2
5,6	Albert, Eric	Expatriate Financial Sector Professional based in China 1, Expatriate Financial Sector Professional Based in China 2	2014	In Person/Informal Discussion	CHN(E)-FSP-1; CHN(E)-FSP-2
7	Wang	Former Chinese Law Enforcement Agent 1	2014	In Person/31.28	CHN-(F)LE-1

Germany (GER)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Bastian	German Cybersecurity Professional 1	2013	In Person/44.27	GER-CSP-1

Hong Kong (HK)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Franklin	Expatriate Cybersecurity Professional Based in Hong Kong 1	2012	In Person/44.14	HK(E)-CSP-1
2	Oscar	Former Hong Kong Law Enforcement Agent 1	2012	In Person/ Unrecorded Interview	HK-(F)LE-1
3	Nathaniel	Hong Kong Cybersecurity Professional 1	2012	In Person/Informal Discussion	HK-CSP-1
4,5	Irving/Win	Hong Kong Prosecutor 1, Hong Kong Prosecutor 2	2012	In Person/Informal Discussion	HK-P-1; HK-P-2
6	Billy	Former Hong Kong Law Enforcement Agent 2	2012	In Person/ Unrecorded Interview	HK-(F)LE-2
7	Jackson	Hong Kong Cybersecurity Professional 2	2012	In Person/Informal Discussion	HK-CSP-2

India (IND)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Rahul	Indian Cybersecurity Professional 1	2015	In Person/25.15	IND-CSP-1
2	Sachin	Indian Cybersecurity Professional 2	2015	In Person/36.32	IND-CSP-2

3	Raj	Former Indian Law Enforcement Agent 1	2015	In Person/32.17	IND-(F)LE-1

Latvia (LAT)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Ivo	Latvian Law Enforcement Agent 1	2015	In Person/38.29	LAT-LE-1
2	Kristiana	Latvian Financial Sector Professional 1	2015	In Person/ Informal Discussion	LAT-FSP-1
3	Artis	Latvian Cybersecurity Professional 1	2015	In Person/30.05	LAT-CSP-1

Malaysia (MY)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1,2	Richard, Issam	Malaysian Law Enforcement Agent 1, Malaysian Law Enforcement Agent 2	2012	In Person/67.48	MY-LE-1; MY-LE-2
3	Amin	Malaysian Cybersecurity Professional 1	2013	In Person/ Unrecorded Interview	MY-CSP-1
4,5	Elisabeth, Firdaus	Malaysian Cybersecurity Professional 2, Malaysian Cybersecurity Professional 3	2013	In Person/ Informal Discussion	MY-CSP-2; MY-CSP-3
6	Irfan	Malaysian Cybersecurity Professional 4	2013	In Person/64.23	MY-CSP-4
7	Haziq	Malaysian Law Enforcement Agent 3	2013	In Person/ Unrecorded Interview	MY-LE-3
8	Kelvin	Malaysian Hacker 1	2015	In Person/48.11	MY-H-1

Netherlands (NLD)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1,2	Dingeman, Christian	Dutch Law Enforcement Agent 1, Dutch Law Enforcement Agent 2	2014	In Person/53.34	NLD-LE-1; NLD-LE-2
3	Daniel	Expatriate Cybersecurity Professional Based in the Netherlands 1	2014	In Person/36.43	NLD(E)-CSP-1

4	Rafael	Dutch Cybsercurity Professional 1	2014	In Person/49.26	NLD-CSP-1

Nigeria (NIG)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Gideon	Nigerian Cybersecurity Professional 1	2016	In Person/ Unrecorded Interview	NIG-CSP-1
2,3,4,5	Samuel, Olawale, Micah, Godwin	Nigerian Law Enforcement Agent 1, Nigerian Law Enforcement Agent 2, Nigerian Law Enforcement Agent 3, Nigerian Law Enforcement Agent 4	2016	In Person/ Unrecorded Interview	NIG-LE-1; NIG-LE-2; NIG-LE-3; NIG-LE-4
6	Adewale	Nigerian Law Enforcement Agent 5	2016	In Person/ Informal Discussion	NIG-LE-5
7	Solomon	Nigerian IT Professional 1	2016	In Person/80.33	NIG-ITP-1
8	Idris	Former Nigerian Law Enforcement Agent 1	2016	In Person/ Unrecorded Interview	NIG-(F)LE-1
9,10	Sunday, Kingsley	Nigerian Cybersecurity Professional 2, Nigerian Cybersecurity Professional 3	2016	In Person/49.36	NIG-CSP-2; NIG-CSP-3
11	Joseph	Expatriate Journalist based in Nigeria 1	2016	In Person/ Informal Discussion	NIG(E)-J-1
12	Ayo	Nigerian Law Enforcement Agent 6	2016	In Person/ Unrecorded Interview	NIG-LE-6
13	Lawrence	Nigerian Financial Sector Professional 1	2016	In Person/50.10	NIG-FSP-1
14	Chris	Nigerian Financial Sector Professional 2	2016	In Person/51.54	NIG-FSP-2
15	Yinka	Nigerian Cybersecurity Professional 4	2016	In Person/41.53	NIG-CSP-4

Romania (ROM)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Virgil	Former Romanian Law Enforcement Agent 1	2014	In Person/ Unrecorded	ROM-(F)LE-1

				Interview	
2	Alexandru	Romanian Law Enforcement Agent 1	2014	In Person/ Unrecorded Interview	ROM-LE-1
3	Razvan	Former Romanian Law Enforcement Agent 2	2014	In Person/43.38	ROM-(F)LE-2
4	Maria	Romanian Prosecutor 1	2014	In Person/ Unrecorded Interview	ROM-P-1
5	Iulia	Romanian Law Enforcement Agent 2	2014	In Person/Informal Discussion	ROM-LE-2
6	Adrian	Romanian Cybersecurity Professional 1	2015	In Person/ Unrecorded Background Interview	ROM-CSP-1
7	Silviu	Romanian Law Enforcement Agent 3	2015	In Person/ Unrecorded Background Interview	ROM-LE-3
8,9	Dorian, Ionut	Romanian Academic 1, Romanian Hacker 1	2015	In Person/Informal Discussion	ROM-A-1; ROM-H-1
10,11,12	Sophia, Madalin, Cristian	Romanian Journalist 1, Romanian Prosecutor 2, Former Romanian Law Enforcement Agent 3	2015	In Person/ Unrecorded Background Interview	ROM-J-1; ROM-P-2; ROM-(F)LE-3
13	Mihai	Romanian Cybersecurity Professional 2	2015	In Person/ Informal Discussion	ROM-CSP-2
14,15	Marcel, Andrei	Romanian Cybersecurity Professional 3, Romanian Cybersecurity Professional 4	2015	In Person/ Unrecorded Background Interview	ROM-CSP-3; ROM-CSP-4
16	Tiberius	Romanian Prosecutor 3	2015	In Person/ Informal Discussion	ROM-P-3

Russia (RUS)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Anton	Russian Cybersecurity Professional 1	2013	In Person/33.49	RUS-CSP-1
2	Arkady	Russian Cybersecurity Professional 2	2013	In Person/41.02	RUS-CSP-2

3,4	Vladislav, Vasily	Russian Cybersecurity Professional 3, Former Russian Law Enforcement Agent 1	2013	In Person/92.37	RUS-CSP-3; RUS-(F)LE-1
6	Bogdan	Russian Financial Sector Professional 1	2013	In Person/ Informal Discussion	RUS-FSP-1
7	Artyom	Russian IT Professional 1	2013	In Person/14.36	RUS-ITP-1
8	Mikhail	Russian Cybersecurity Professional 4	2013	In Person/39.42	RUS-CSP-4
9	Valery	Russian Financial Sector Professional 2	2013	In Person/ Informal Discussion	RUS-FSP-2
10,11	Vladimir, Aleks	Russian Cybersecurity Professional 5, Russian Cybersecurity Professional 6	2014	In Person/ Unrecorded Interview	RUS-CSP-5; RUS-CSP-6
12	Sasha	Russian Cybersecurity Professional 7	2015	In Person/54.07	RUS-CSP-7
13	Ilya	Russian Cybersecurity Professional 8	2015	In Person/ Unrecorded Interview	RUS-CSP-8
14	Alexei	Russian Cybersecurity Professional 9	2015	In Person/50.47	RUS-CSP-9
15,16,17	Dmitry, Petro, Andrei	Russian Financial Sector Professional 3, Russian Cybersecurity Professional 10, Russian Cybersecurity Professional 11	2015	In Person/ Unrecorded Interview	RUS-FSP-3; RUS-CSP-10; RUS-CSP-11
18	Anatoly	Russian Cybersecurity Professional 12	2015	In Person/35.42	RUS-CSP-12
19	Evgeny	Russian Cybersecurity Professional 13	2015	Phone/21.55	RUS-CSP-13

Singapore (SGP)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Geoff	Expatriate Hacker Based in Singapore 1	2012	In Person/51.38	SGP(E)-H-1
2	Alvin	Former Singaporean Prosecutor 1	2012	In Person/31.46	SGP-(F)P-1
3	Raymond	Singaporean Cybersecurity Professional 1	2012	In Person/28.39	SGP-CSP-1
4	Vincent	Former Singaporean Law Enforcement Agent 1	2012	In Person/ Informal Discussion	SGP-(F)LE-1

5	Adrian	Former Singaporean Law Enforcement Agent 2	2013	Phone/20.32	SGP-(F)LE-2
6	Andrew	Singaporean Cybersecurity Professional 2	2015	In Person/41.02	SGP-CSP-2

Switzerland (SWI)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Denis	Swiss Cybersecurity Professional 1	2013	In Person/41.58	SWI-CSP-1
2	Victor	Expatriate Cybersecurity Professional based in Switzerland 1	2013	In Person/44.24	SWI(E)-CSP-1

Thailand (THA)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Jerome	Expatriate Cybersecurity Professional based in Thailand 1	2014	In Person/39.47	THA(E)-CSP-1
2	Kittinan	Thai Cybersecurity Professional 1	2014	In Person/ Informal Discussion	THA-CSP-1
3,4	Sirawit, Adisak	Thai Law Enforcement Agent 1, Thai Law Enforcement Agent 2	2014	In Person/34.02	THA-LE-1; THA-LE-2

United Kingdom and Ireland (UK/IRE)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Jennifer	Irish Cybersecurity Professional 1	2011	Phone/16.10	IRE-CSP-1
2	Nithan	British Cybersecurity Professional 1	2011	In Person/48.27	UK-CSP-1
3	Alex	Former UK Law Enforcement Agent 1	2011	In Person/44.50	UK-(F)LE-1
4	Phillip	Former UK Law Enforcement Agent 2	2011	In Person/63.03	UK-(F)LE-2
5	Tom	UK Law Enforcement Agent 1	2011	Phone/54.15	UK-LE-1
6	Amber	Expatriate IT professional based in the UK 1	2011	In Person/ Informal Discussion	UK(E)-ITP-1

7	Edward	UK Prosecutor 1	2011	In Person/ Informal Discussion	UK-P-1
8	Jake	British Cybersecurity Professional 2	2013	Phone/26.56	UK-CSP-2
9,10,11	Frank, Luke, Daisy	British Cybersecurity Professional 3, Expatriate Cybsercurity Professional based in the UK 1, Expatriate Cybsecurity Professional based in the UK 2	2013	In Person/ Informal Discussion	UK-CSP-3; UK(E)-CSP-1; UK(E)-CSP-2
12	Nigel	British Financial Sector Professional 1	2014	In Person/43.50	UK-FSP-1
13	Elenor	Former UK Law Enforcement Agent 3	2014	In Person/30.45	UK-(F)LE-3
14	Peter	Former UK Law Enforcement Agent 4	2014	In Person/50.53	UK-(F)LE-4
15	Craig	British Cybersecurity Professional 4	2014	In Person/73.31	UK-CSP-4
16	Brendan	British Cybersecurity Professional 5	2014	In Person/28.16	UK-CSP-5
17	Owen	Former UK Law Enforcement Agent 5	2015	In Person/84.22	UK-(F)LE-5
18	Jason	Former UK Law Enforcement Agent 6	2015	In Person/ Informal Discussion	UK-(F)LE-6
19	Trevor	UK Law Enforcement Agent 2	2015	In Person/29.57	UK-LE-2
20	Paul	British Cybersecurity Professional 6	2015	In Person/40.11	UK-CSP-6
21	Colin	UK Law Enforcement Agent 3	2015	In Person/54.19	UK-LE-3
22	Connor	British Cybersecurity Professional 7	2015	In Person/35.56	UK-CSP-7
23	Angus	British Financial Sector Professional 2	2015	In Person/ Informal Discussion	UK-FSP-2
24	Jay	UK Prosecutor 2	2015	In Person/ Informal Discussion	UK-P-2
25	Cameron	British Financial Sector Professional 3	2015	Phone/Informal Discussion	UK-FSP-3
26	Spencer	British Cybersecurity Professional 8	2016	Phone/51.54	UK-CSP-8

Ukraine (UKR)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Artem	Former Ukrainian Law Enforcement Agent 1	2015	Written Communication	UKR-(F)LE-1
2	Dima	Ukrainian IT Professional 1	2015	In Person/ Informal Discussion	UKR-ITP-1
3	Sergey	Ukrainian Law Enforcement Agent 1	2015	In Person/29.41	UKR-LE-1
4	Keith	Expatriate Cybersecurity Professional based in Ukraine 1	2015	In Person/68.16	UKR(E)-CSP-1
5	Maksym	Ukrainian Cyberscurity Professional 1	2015	In Person/ Unrecorded Interview	UKR-CSP-1
6	Oleg	Ukrainian Cyberscurity Professional 2	2015	In Person/ Unrecorded Interview	UKR-CSP-2
7	Nikita	Former Ukrainian Law Enforcement Agent 2	2015	In Person/56.22	UKR-(F)LE-2
8	Kirill	Ukrainian Law Enforcement Agent 2	2015	In Person/20.33	UKR-LE-2
9	Misha	Former Ukrainian Law Enforcement Agent 3	2015	In Person/ Unrecorded Interview	UKR-(F)LE-3
10	Igor	Ukrainian Cybersecurity Professional 3	2015	In Person /Unrecorded Interview	UKR-CSP-3

United States (US)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Olivia	American Cybersecurity Professional 1	2012	In Person/34.39	US-CSP-1
2	Ethan	Former US Law Enforcement Agent 1	2012	Phone/35.26	US-(F)LE-1
3	William	Former US Law Enforcement Agent 2	2012	In Person/36.08	US-(F)LE-2
4	Ryan	American Cybersecurity Professional 2	2012	In Person/54.59	US-CSP-2
5	Michael	Former US Law Enforcement Agent 3	2012	In Person/37.33	US-(F)LE-3
6	Matthew	Former US Law Enforcement Agent 4	2012	In Person/41.07	US-(F)LE-4

7	Jacob	American Cybersecurity Professional 3	2012	In Person/62.29	US-CSP-3
8	Aiden	Former US Prosecutor 1	2012	In Person/26.53	US-(F)P-1;
9	Nathan	Former US Law Enforcement Agent 5	2012	In Person/40.42	US-(F)LE-5
10	Caleb	Former US Prosecutor 2	2012	In Person/20.15	US-(F)P-2;
11	Samantha	Former US Prosecutor 3	2012	In Person/9.48	US-(F)P-3;
12	Adam	Former US Law Enforcement Agent 6	2012	In Person/26.58	US-(F)LE-6
13	Jordan	American Cybersecurity Professional 4	2012	In Person/60.29	US-CSP-4
14	Benjamin	American Cybersecurity Professional 5	2012	In Person/54.40	US-CSP-5
15	Jeremy	American Cybersecurity Professional 6	2012	In Person/58.28	US-CSP-6
16	Gavin	American Cybersecurity Professional 7	2012	In Person/34.57	US-CSP-7
17	Logan	American Cybersecurity Professional 8	2012	In Person/45.58	US-CSP-8
18	Anne	US Prosecutor 1	2012	In Person/ Informal Discussion	US-P-1
19	Lucas	US Law Enforcement Agent 1	2012	In Person/ Unrecorded Interview	US-LE-1
20	Eugene	American Cybersecurity Professional 9	2012	In Person/24.05	US-CSP-9
21	Alexander	Former US Law Enforcement Agent 7	2012	In Person/55.5	US-(F)LE-7
22	John	Expatriate Cybersecurity Professional based in America 1	2012	Phone/16.37	US(E)-CSP-1
23	Dylan	American Cybersecurity Professional 10	2013	Phone/32.59	US-CSP-10
24	Jed	US Prosecutor 2	2013	Phone/40.17	US-P-2;
25	Carter	US Law Enforcement Agent 2	2013	Phone/53.34	US-LE-2
26,27	Christopher, Wyatt	American Cybersecurity Professional 11, American Cybersecurity Professional 12	2013	Phone/46.41	US-CSP-11; US-CSP-12
28	Joshua	American Cybersecurity Professional 13	2013	Phone/28.57	US-CSP-13
29	Abbie	Former US Prosecutor 4	2013	In Person/53.41	US-(F)P-4;

30	Scarlett	American Cybersecurity Professional 14	2013	In Person/57.24	US-CSP-14
31	Andy	American Journalist 1	2013	In Person/ Informal Discussion	US-J-1
32	Jack	US Law Enforcement Agent 3	2013	In Person/50.28	US-LE-3
33,34	Rick, Simon	US Law Enforcement Agent 4, US Law Enforcement Agent 5	2013	In Person/ Informal Discussion	US-LE-4; US-LE-5
35	Landon	Former US Law Enforcement Agent 8	2014	In Person/93.30	US-(F)LE-8
36	Elijah	Former US Prosecutor 5	2014	In Person/37.20	US-(F)P-5;
37,38	Danielle, Leo	US Law Enforcement Agent 6, US Law Enforcement Agent 7	2014	In Person/38.29	US-LE-6; US-LE-7
39	Ryder	US Law Enforcement Agent 8	2015	Phone/ Unrecorded Interview	US-LE-8
40	Clark	US Law Enforcement Agent 9	2016	Phone/31.07	US-LE-9

Redacted or Undisclosed (INT/UDL)

No.	*Alias*	*Description*	*Year*	*Type*	*Code*
1	Neville	International Organisation Officer 1	2013	Phone/20.51	INT-OO-1
2	Florian	International Organisation Officer 2	2013	In Person/34.23	INT-OO-2
3	Timothy	International Organisation Officer 3	2013	In Person/16.33	INT-OO-3
4	Rikard	Cybersecurity Professional (Undisclosed Location/Nationality) 1	2013	Written Communication	UDL-CSP-1
5	Patrice	International Organisation Officer 4	2015	In Person/ Unrecorded Interview	INT-OO-4
6	Slavoj	International Organisation Officer 5	2015	In Person/59.20	INT-OO-5
7	Vincent	International Organisation Officer 6	2015	In Person/34.40	INT-OO-6

Former Cybercriminals (NA/EE/SEA/WE)

No.	*Alias*	*Description*	*Type*	*Code*
1	Jeremy	Former Western European Hacker 1	In Person/38.56	WE-(F)H-1
2	Sean	Former Western European Cybercriminal 1	In Person/73.01 and Written Communication	WE-(F)CC-1
3	Dave	Former Expatriate Cybercriminal Based in Southeast Asia 1	In Person/68.22	SEA(E)-(F)CC-1
4	Noah	Former North American Cybercriminal 1	In Person/37.25	NA-(F)CC-1
5	Ahmed	Former Southeast Asian Cybercriminal 1	Phone/Unrecorded Interview	SEA-(F)CC-1
6	Casper	Former Western European Cybercriminal 2	In Person/43.56	WE-(F)CC-2
7	Scott	Former North American Cybercriminal 2	Written Communication	NA-(F)CC-2
8	Claudiu	Former Eastern European Cybercriminal 1	In Person/ Informal Discussion	EE-(F)CC-1
9	Lance	Former North American Cybercriminal 3	Phone/50.47	NA-(F)CC-3
10	Don	Former North American Cybercriminal 4	Written Communication	NA-(F)CC-4
11	Fyodor	Former Eastern European Cybercriminal 2	Written Communication	EE-(F)CC-2
12	Jim	Former North American Cybercriminal 5	Written Communication	NA-(F)CC-5