CYBERCRIMES@GAMBLING_SITES.COM

By

Aunshul Rege

A Thesis Submitted to
Saint Mary's University, Halifax, Nova Scotia
in Partial Fulfillment of the Requirements for
the Degree of Masters of Arts in Criminology

June 2008, Halifax, Nova Scotia

Approved:	Dr. John McMullan Supervisor
Approved:	Dr. David Perrier Reader
Approved:	Dr. Kerry Chambers External Examiner
Date:	June 12th, 2008

Library and
Archives Canada

Published Heritage
Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et
Archives Canada

Direction du
Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-44662-1
Our file Notre référence
ISBN: 978-0-494-44662-1

CYBERCRIMES@GAMBLING_SITES.COM

Aunshul Rege, June 12, 2008

ABSTRACT

Online gambling sites have proliferated exponentially since the mid-1990s generating billions of dollars in revenue annually. However, this successful global industry is frequently the target or the perpetrator of cybercrime, which pose serious problems for gambling operations and players worldwide. This thesis explores cybercrimes at gambling websites, focusing on the organizational dynamics of crime, criminality, and criminal communication. I draw on theories of criminal organization and cyberspace to develop an integrated theory that accounts for how criminals organize, operate, and network in digital environments around the six dimensions of space, time, movement, scope, structure, and preservation.

I employ a document analysis methodology for this thesis, by examining gambling commission reports, journal articles, newspaper and magazine articles, security archives, technical white papers, and "how-to-do-it" hacker manuals. Documents published between 1996 and 2008 are collected from the internet, university libraries, and journal databases, and this data is coded around seven intersecting areas: internet gambling and cybercrime; organized crime, cyberextortion, and money laundering; hacking and cracking; cheating and collusion; fraud, non-payment of winnings, and software tampering; underage gambling; social control measures against cybercrime.

I find that cybercrimes occurring at gambling sites involve a variety of criminals and an assortment of digitized techniques, both of which range in their organizational sophistication. I argue that while my integrated theoretical framework adequately captures crimes and criminality occurring exclusively in cyberspace, it requires modification along the concepts of space, time, and structure to address the organizational traits of crimes and criminals in 'hybrid' space. I then evaluate my revised integrated theory along the criteria of scope, coherence, causality, and predictive power to demonstrate theoretical growth. Finally, I offer a theoretical proposition that can be used as a point of departure for future cybercrime studies in the criminological discipline.

ACKNOWLEDGEMENTS

The author recognizes the following people for their contributions in the completion of this thesis:

First of all, I was extremely privileged to have Dr. John McMullan as my guru. His guidance, encouragement, commitment, and patience as I progressed through this intellectual endeavor were immensely beneficial. For all that I have learned from him, and for all his faith in me, I will forever be in his debt. I was also fortunate to have Dr. David Perrier as a member of my thesis committee. He was a constant source of motivation and held a genuine interest in my success. This project would not have been completed without the support of these two mentors.

I also thank my parents, husband, and brother for their love, affection, and support throughout this research project. They were my cheering squad, always making me believe in myself. Were it not for their dedicated encouragement, this project would not have been possible.

I thank Saint Mary's University and the Social Science and Humanities Research Council of Canada for their generous fellowships, which allowed me to concentrate fully on my thesis.

Finally I thank my friends Delthia Miller, Jessica Chubb, Julie-Ann Vincent, Kathryn Bliss, Matthew Johnson, and Steve Ciccolella for believing in my abilities and supporting me through the various stages of my research. I thank Dr. Westhaver and Dr. Crocker for their suggestions and assistance, as well as Lindia Smith and Sandi Cole-Pay, who were extremely helpful and supportive. I also thank Mr. Promaine, Ms. Sanderson, Mr. Sisk, and Mr. Whiting for their confidence in me.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

Chapter 1

Introduction

Computers and technology have impacted our society tremendously. The fusion of computing and communications has resulted in the creation of cyberspace that transcends the physical domain. The possibilities brought forth by cyberspace and information and communications technologies (ICTs) now allow individuals to accomplish conventional tasks with minimal spatial-temporal constraints. Not only is this virtual space a rich source of information, knowledge, and interaction, but it also houses online communities, shops, and industries.

The gambling industry is one that has benefited from these technological developments. Five factors make online gambling attractive to customers. First, gamblers do not have to leave their homes or workplaces to play and wager. Gambling sites are open for business 24 hours a day, 7 days a week, allowing customers to play remotely at their convenience (Cabot 2001, p. 42). Second, online services have become more affordable over the years because technological advances have produced more efficient, faster, and cheaper computer systems, which, in turn, have made online gambling services cheaper than more traditional forms of gambling (Griffiths 2003, p.559). Third, the anonymity feature of the internet allows customers to participate privately in gambling without the oversight of others or the "fear of stigma" (Griffiths 2003, p. 559). Fourth, interactive online applications, such as emails and newsgroups, offer a convenient forum to engage in gambling activities. Customers receive constant information about new gambling sites and games, and thus participate in a wide variety of games of their choice. Finally, other technological developments – sophisticated gaming software,

integrated digital-cash systems, live remote wagering, and increased realism offer convenient, attractive websites to play and stay on. Not surprisingly, these qualities have resulted in the proliferation of the online gambling sector, so much so that there are nearly 300,000 unique gaming sites, of which only 14% are licensed (CERT-LEXSI 2006, p. 4). These sites offer an assortment of gambling services, such as lotteries, casino games, bingo, sports betting, and card games (BCPRG 2004, p.1; Stewart 2006, p. 2). The flourishing online gambling industry generates over 15 billion dollars in known revenues every year and an estimated several billion dollars in unreported profit (CERT-LEXSI 2006, p. 3).

Not surprisingly, these sites are prime targets for cybercrime, both on a daily basis and during peak betting periods such as the SuperBowl, the Grand National, and other major sporting events. ICTs have also enabled conventional crimes to shift online, making them easier to commit; stalking, terrorism, and extortion are now conducted in the parallel dimension of cyberspace. Furthermore, virtual space has given rise to completely new crimes, such as hacking and the creation of malware (malicious software) that are specific to this new spatial configuration. Computer viruses, which were first used by hackers for the sole purpose of acquiring fame, are now being used in the "biological warfare of cyberspace" exploiting the information economy (Whitaker 1999, p. 70). Cyberspace is borderless and has a global existence, which makes it a difficult medium to regulate. As cybercrime is a new and rapidly increasing phenomenon, policing, regulatory, and legal bodies have not yet caught up, giving cybercriminals the upper hand in digital worlds.

Cybercrime has now received attention from online businesses and law

enforcement authorities, yet it has no clear or single definition. The Canadian Police College and RCMP's Integrated Technological Crime Unit (ITCU) suggest two general types of cybercrime: (i) those using technology, the internet, and ICT applications as instruments/tools to facilitate or commit crimes, such as credit card fraud, spam, and software piracy, and (ii) those victimizing ICT applications utilizing technology and the internet, such as hacking and extortion (LeBeuf 2001, p. 6; RCMP 2007, p. 2). Smith (2003) expands this definition to include crimes where ICTs are incidental, yet used in the commission of crime, and Symantec (2007a) defines cybercrime as any crime (i) where ICTs may be the agent/perpetrator, the facilitator/instrument, or the victim/target of the crime and (ii) which may be either a single event or an on-going series of events. I subscribe to Symantec's (2007a) definition because it encompasses both the duration of the crime, as well as the roles (perpetrator, facilitator, victim) of ICTs in cybercrimes. I define cybercriminals as offenders who (i) are driven by a range of motivations, such as thrill, revenge, and profit, (ii) commit and/or facilitate cybercrimes, (iii) work alone, in simple partnerships, or in more formalized settings, and (iv) have varying levels of technical expertise (Weaver, Paxson, Staniford & Cunningham 2003; Warner 2001; Datz 2004; Krone 2005; Brenner 2002; Wall 2007; Rogers 2005). In the context of my research, the category of cybercriminals not only includes hackers, cheaters, money launderers, and extortionists, but also gambling site operators and managers, as they perpetrate cybercrimes against their customers, licensees, and competitors.

Research Problem and Questions

An assortment of research has been conducted on internet gambling (Shaffer 1996; Griffiths 1994; Korn 2000; Mitka 2001; Ladd & Petry 2002; Griffiths & Wood

2000; Derevensky, Gupta & Magoon 2004; Clarke 2003; Makela 2000; Fabiansson 2006; Kish 1999; Keller 1999; Andrle 2006; Clarke & Dempsey 2001; Dewar 2001), and on cybercrime (Chandler 1996; Duff & Gardiner 1996; Jordan & Taylor 1998; Krone 2005; Hafner & Markoff 1995; Mann & Sutton 1998; Denning 2000; Williams 2002; Brenner 2002; Paulson & Weber 2006; Goodell 1996; Speer 2000; Michalowski & Pfuhl 1991; Littman 1995; Schwartau 2000), but these two bodies of knowledge have rarely intersected in social science research. Research on cybercrimes at gambling sites is still in its infancy and is either descriptive in nature (Kvarnstrom, Lundin & Jonsson 2000; Cabot 2001), or focuses on the consequences of cybercrime rather than its organizational dimensions (Chen et al. 2005; McMillen & Grabosky 1998; Zacharias 2004). Furthermore, these crimes have been studied in isolation; for instance, studies have either addressed collusion (Smed, Knuutila & Hakonen 2006), or cyberextortion (Paulson & Weber 2006), or fraud (Kelley, Todosichuk & Azmier 2001), thereby ignoring the overall phenomenon of cybercrimes at gambling sites and how these crimes intersect. The organizational dynamics of cybercrimes at gambling sites and the role of ICTs in the organization of cybercriminals remains undeveloped (Ranade, Bailey & Harvey 2006; McMullan & Rege 2007).

My thesis addresses this gap by examining how cyberspace and ICTs shape criminal technique, organization, and communication; it explores how digital environments alter conventional notions of structure, membership, and criminality, and how cybercriminals use ICTs to evade, avoid, counter, and negotiate the actions taken by governments, security firms, and gambling providers to curb cybercrime. Gambling sites are subjected to extortion, fraud, player collusion, hack-attacks, and money laundering,

and this plethora of cybercrimes make gambling sites ideal venues to situate my research and examine the organizational dynamics of cybercrime by asking: How are gambling sites victims of cybercrimes? How do gambling sites, in turn, facilitate and perpetuate the commission of cybercrimes? How do ICTs impact criminal organizations, their communication, and techniques? What advantages are offered by the digital environment to cybercriminals? How do cybercriminals benefit from the challenges faced by law enforcement and security agents? What proactive and reactive techniques are used by cybercriminals to successfully circumvent policing and legal threats?

Significance of Research

Researching cybercrime and cybercriminals is an important endeavor, as technologically-dependant societies are negatively affected by them. It is therefore imperative to understand this new breed of criminal and how they operate. The literature on cybercrime at gambling sites, however, is still in its infancy. While some studies have explored cybercrimes at gambling sites, they have been conducted by technological researchers and gaming industries, and are hence too narrow in nature; they do not examine cybercrimes through a sociological lens. Furthermore, the studies on online gambling and cybercrime are found in isolation; this disconnect hinders a thorough understanding of criminal activity at gambling sites. The present study therefore builds on the existing literature in online criminality and gambling, and draws them together to make new points of contact. By doing so, this research serves to stimulate new ways of thinking about cybercriminals and how they commit crimes at gambling sites.

This study fills an important gap in criminological theory. Conventional theories for criminal organization were created before the advent of cyberspace and technology,

and have therefore not considered their impact on the organization of criminals. This research offers a preliminary examination of online criminal structure using a socio-organizational level of analysis. It transcends conventional typologies and models of criminal organization and offers an integrated theoretical framework that examines how digital environments influence cybercriminal organization. It proposes a new typology of online criminal organization, focusing on its fluid, dynamic, and transient nature. This integrated theory and typology can be used for future research that also examines cybercriminal organization operating in different contexts.

This study is also significant from a methodological perspective. It employs a systematic procedure to explore the elusive, covert, and dynamic phenomenon that makes up cybercrimes at gambling sites. It connects a wide range of documents: 'how to do it' hacking manuals and hacker interviews, journal articles and academic texts on cybercrimes, government reports and security white papers, and media cases. This connection develops a dialogue between the different knowledge bases; it offers new insights and multiple perspectives, which captures the different instances of cybercrimes at gambling sites. Additionally, this methodology may serve as a guideline for future studies directed at other online institutions, such as banks, stock markets, and shops; it can be tailored to reflect the websites and cybercrimes being examined.

A missing ingredient in cybercrime studies is the study of the cybercrime itself. Most accounts of cybercrimes are descriptive or technical, and not socio-organizational. Research has typically focused on how cybercriminals evade external threats by altering their organizational dynamics. This study goes further and examines the anatomy of criminal techniques, their characteristics, and how the attacks themselves are structured

to circumvent policing and security threats. Furthermore, this study links each type of criminal organization to different criminal techniques, thereby revealing how criminal organization determines the attack, and vice versa. These findings contribute to understanding the continually changing nature of criminal organization and operation in cyberspace.

Finally, this study is also important to the field of internet gambling studies as it examines cybercrime at gambling sites, an area where research has been scarce. By identifying the assortment of virtual crimes at gambling sites and creating a typology of these crimes, my research addresses the prevalence of cybercriminality, and the benefits offered to cybercriminals, at and by online gambling environments. My exploratory research can be used as a foundation for more specific studies into the area of cybercrime at gambling sites. Furthermore, by examining how cybercriminals exploit gambling site vulnerabilities, manipulate gaming programs, and circumvent protective measures, this thesis contributes to the areas of internal and external security issues in the gambling industry.

Thesis Structure

This study is organized into six chapters. The next chapter introduces the theoretical perspectives that guide this study in understanding online criminal organization and operation. Specifically, I draw from (i) Deleuze and Guattari's (1987) concepts of smooth and striated spaces, nomadology, deterritorialization, and reterritorialization, as well as Baudrillard's (1988) theory of the hyperreal, to account for the characteristics of cyberspace and notions of identity, and (ii) Best and Luckenbill's (1982) taxonomy of criminal organization and Chambliss' (1978), Smith's (1974),

Albini's (1971), and Lemieux's (2003) network-based models of organized crime to serve as a guideline for examining online criminal organization. I combine these two theoretical bodies to develop an integrated theoretical framework that I then use to develop a cybercriminal typology.

The purpose of chapter three is to explain the research methods that address my questions. Here I define document analysis and expound on the use of the internet and the Google search engine for conducting my research. I discuss how I sample approximately five hundred articles over a thirteen-year time frame (1996-2008), which range from company reports, financial reports, gambling commission reports, academic and journal articles, newspaper and magazine articles, legal cases, and hacker testimonials. Then I detail my systematic data collection protocols and coding strategies, which I use to filter and organize raw data. Finally, I identify and address the methodological limitations of my study.

Chapter four presents my findings on the modus operandi of cybercriminals. I discuss various criminal techniques that range in sophistication and expertise. I examine how cybercriminals exploit, manipulate, and intercept gambling site operations and data flow. I also examine the use of malware (malicious software), hacking toolkits, artificial intelligence, and 'bot-networks' in the execution of cybercrimes. I then discuss how cybercriminals use fake and cloned gambling sites to trick customers or launder money. I use several case studies to illustrate the design and implementation of each digital technique, the technical skills and knowledge required, and how each technique is useful for different types of criminal activity at gambling sites.

In chapter five, I present my findings on the organizational dynamics of various types of cybercrimes. I draw on several case studies to examine how criminals organize themselves in digital environments, addressing solo operations, alliances, and elaborate networks. I examine how criminal organization is context-specific and dynamic, depending on the type of criminal activity and its duration. Specifically, I focus on the size of the criminal network, division of labour, the nature and duration of memberships, the life-spans of criminal organizations, the types of digital attacks used, techniques used to avoid, evade, or neutralize policing and security threats, and the motivations and rationales of cybercriminals.

Finally, I offer an interpretation of my findings in chapter six. I demonstrate how my integrated theory captures the organization of crime and criminality in cyberspace exclusively. Then, I discuss some limitations of my theoretical framework in accounting for the organizational dynamics of cybercrime in both physical and online environments. I remodel my integrated theory to refine three dimensions: space, time, and criminal structure, and improve my theoretical framework so that it expands the scope, coherence, causality, and predictive power of explanation. I conclude my thesis by recommending four areas for future research made evident by my study.

Chapter 2

Towards a Theory of Cybercrime Organization

Introduction

In this chapter, I examine theories of cyberspace and theories on criminal organization and organized crime to create an integrated theoretical framework that aids me in understanding criminal activity at gambling sites. First, I outline Deleuze and Guattari's (1987) concepts of smooth and striated spaces and use these to account for the dynamics and characteristics of cyberspace. Second, I address the nature of smooth space using Deleuze and Guattari's (1987) rhizomatic model, as this is the space in which cybercriminals operate. I discuss the key ideas and principles that inform this model: connectivity, heterogeneity, multiplicity, regeneration, decalcomania, cartography, nomadology, and lines of flight, and their relevance to understanding digital environments and the nomadic movement of cybercriminals in this terrain. Third, I examine the implications of cyberspace on notions of community, identity, and territory. I review the literature and discuss the concepts of 'virtual communities' (Oldenburg 1989; Rheingold 1993), 'hyperreality' (Baudrillard 1988), 'interpellations' (Poster 1995), 'pluralism' (Turkle 1997), and 'deterritorialization' and 'reterritorialization' (Deleuze & Guattari 1987; Wenninger 2007), and discuss how they are useful to my thesis. Fourth, I review the literature on criminal organization and organized crime to identify the theoretical features and intersections most suited for understanding internet crime. In particular, I examine Best and Luckenbill's (1982) typology of criminal organization, Chambliss' (1978) Crime Network model, Smith's (1974) Enterprise model, Albini's (1971) Patron-Client model, and Lemieux's (2003) Crime Network model to identify

factors that determine the characteristics of the different organizational typologies in order to apply these to online criminal organization. Finally, I develop an integrated theoretical framework that demonstrates how cyberspace impacts six dimensions of criminal organization, and propose a new typology for online criminal organization. I conclude by raising several research questions that stem from this integrated theoretical framework.

The Space of Cyberspace

Deleuze and Guattari (1987) use the terms *smooth* and *striated* to conceptualize space. Smooth spaces are heterogeneous and dynamic spaces which allow movement in a multiplicity of directions without any restrictions. They are fluid spaces of continuous transformation and best thought of as open-ended, informal, and amorphous. Smooth spaces are *rhizomatic*; "regions are juxtaposed without reference to an overarching metric principle or directionality" (Patton 2000, p. 112). Smooth space, however, is not necessarily freer or truer, but a space where *things are different* (Deleuze & Guattari 1987, p. 500; Bayne 2004, p. 303). Cyberspace exists "nowhere and everywhere, it is … constantly being constructed and reconstructed, written and rewritten, by the simultaneous interaction of all those networking in the medium" (Whitaker 1999, p. 55). These characteristics allow cyberspace to harbour *nomadic* and unbounded movement along multiple trajectories or *lines of flight*, giving internet users greater ease and flexibility in their online browsing experience (Herman & Sloop 2000).

In contrast to smooth spaces, striated spaces are bordered, sedentary, and structured. In striated space, "one closes off a surface and 'allocates' it according to determinate intervals, [and] assigned breaks" (Deleuze & Guattari 1987, p. 481).

Hierarchy, rules, control, and boundaries characterize these spaces. As Light and Smith (1998) note, these spaces are codified, gridded, and subjected to concepts, where the prospects for movement are limited (p. 271). Thus, striated spaces force a path for their inhabitants; they are marked by enclosures (nodes) and paths (lines) between these enclosures. Some researchers view the web as a "closed and hierarchical space of striation, destined by its very structure to undermine any attempt to use its spaces" for dynamic thought (Myers 1995). For instance, gambling sites are structured; they offer specific games with predetermined rules for players, which limit their movement, and are protected via firewalls, which, in turn, enclose their sites from external use.

Deleuze and Guattari (1987), however, note that smooth and striated spaces do not exist in pure form: these spaces "exist only in mixture: smooth space is constantly being translated, transversed into a striated space; striated space is constantly being reversed, returned to a smooth space" (p. 474; Moulthrop 1994; Bogard 2000). This relationship exists on a continuum; the spaces that have fewer interruptions (striations) are at the smooth end of the spectrum, while those that are less often reversed are at the striated end. Thus in this sense, space is not a state of being, but a state of *becoming* (Light & Smith 1998, p. 271). Striations continually organize the open (smooth) space, and growth disorganizes and smoothes closed space, so that both these spaces are in a constant state of flux and conflict (Conte 1997, p. 59).

Nunes (1999) views cyberspace as both striated and smooth; striated cyberspace is seen as a "system of regulated connections between determined points on dedicated lines", while smooth cyberspace is a fluid and continuous passage (p. 61). Indeed, how the web is used and conceived construes it as a smooth and/or striated space. The web's

openness, its instability and tendency to change, its "unmappability", and the "unknowability inherent to its vastness" make it smooth, while simultaneously harbouring striated elements, such as virtual communities, stores, security systems, and banks that restrict movement and exercise control through registration, access, monitoring, and assessment (Bayne 2004, p. 306). While cyberspace can be manifested as smooth space, its networked architecture, which relies on centralized control structures, predisposes it as a striated surface as well. I share Nune's (1999) and Bayne's (2004) view of cyberspace as an arena where smoothness and striation interact. I locate my work in this conflict between smooth spaces, which are used by cybercriminals, and striated spaces, which are used by gambling sites and social control agencies. In particular I ask: How do these spaces interact in the context of cybercrimes at gambling sites? How does this tension impact criminal organization and operation in cyberspace? As my thesis focuses on online criminal organization, I now examine smooth (rhizomatic) spaces, because this is the environment where criminals move, organize, and operate to overcome the striations in cyberspace.

Rhizomes, Nomads, and the Internet

Deleuze and Guattari (1987) contrast *arbolic* thought processes with *rhizomatic* ones. They describe arbolic thought as linear, hierarchic, static, and structured; it is "vertical and stiff" (Wray 2003, p.3). Striated space is associated with arbolic thought. Alternatively, rhizomatic thought is non-linear, horizontal, anarchic, nomadic, and is associated with smooth space. Rhizomatic thought moves in multiple directions and can be linked to several other lines of thought (nodes); thus it is multiplicitous in nature. It builds connections between several nodes by multiplying through a process of "lateral

spreading", resulting in a decentralized assemblage with "seemingly endless permutability" (Hodgson & Standish 2006, p. 567). Rhizomatic structures have no centre of origin, what exists is only the inbetween (Lort 2000, p. 1). Deleuze and Guattari (1987) offer six principles of the rhizomatic model: connectivity, heterogeneity, multiplicity, regeneration, decalcomania, and cartography [Figure 1].

The first principle of connectivity suggests that "any point of a rhizome can be connected to anything other, and must be" (Deleuze & Guattari 1987, p. 7). In short, the rhizomatic system is not hierarchical, as a node can be connected to any other node in the system; no node comes before another, nor must it be linked to any specific point. The second principle of heterogeneity states that nodes are not necessarily connected to other nodes sharing similar traits. The internet is an example of a rhizomatic entity where any computer system can link to another networked system on the internet using information 'packets' through which they communicate. Computers do not have to be linked in any particular sequence or hierarchy, and can connect to a variety of other computers, servers, databases, or networks in cyberspace.

The third principle of multiplicity states that an assortment of different nodes can be linked together in numerous ways. As Deleuze and Guattari (1987) note, a rhizomatic system does not have any beginnings or ends; nodes are linked via multiple lines. This multiplicity spreads out "roots and branches [of thought], thereby pluralizing and disseminating, producing differences and multiplicities, [and] making new connections" (as cited in Wray 2003, p. 4). While internet users do not physically move from one node to another, in cyberspace they connect to different websites remotely. As Hamman (1996) notes, users move along multiple lines, and connections between web pages can be

generated intermittently. A connection does not exist until an internet user chooses to make it. Users can view a website and then link to other websites, thereby spreading, pluralizing, and flat lining their 'browsing' or 'surfing' experience.

The fourth principle is regeneration. A rhizome can be "broken, shattered at a given spot, but it will start up again on one of its old lines, or on new lines" (Deleuze & Guattari 1987, p. 9). Thus, an interconnected network can mobilize and manipulate movements and flows around any disruptions. Rhizomes operate by "variation, expansion, conquest, capture, [and] offshoots" (Deleuze & Guattari 1987, p. 21). They exhibit renewal qualities as a broken sub-component can quickly be recreated elsewhere in the network to ensure its persistent existence. This regenerative trait further enhances the principle of multiplicity as new connections and lines are generated over and over again. Websites, for example, manage to create other lines and connections to bypass disrupted lines of information flow, thereby exhibiting the principle of regeneration. For instance, an illegal gambling site may be shut down by internet service providers or law enforcement bodies only to resurface at another location or under a different name.

The fifth and sixth principles of a rhizomatic system are decalcomania and cartography. The decalcomania principle insists that rhizomes do not follow any structural model; they are decentered, informal, and without much structure. The internet, in this sense, has little fixed structure; it is forever changing and modifiable, which may allow net surfers to operate in a fluid and flexible manner. The principle of cartography suggests that the rhizome is a map, which is "open and connectable in all of its dimensions; it is detachable, reversible, [and] susceptible to constant modification" (Deleuze & Guattari 1987, p. 12). Additionally, these maps have multiple points of entry,

which further promote multiplicities and pluralities in the rhizomatic system. Indeed, the internet functions as a map where users worldwide can connect via multiple points of entry, which are scattered around the world. They create maps by linking through dynamic routes, instead of tracing over pre-existing lines (Hamman 1996, p. 4).

These six principles are exhibited by the smooth component of cyberspace, which has no beginning or end, no hierarchy of computers, no sequence of linkages between computers, databases, or other networked systems, and no centralized system of control. This space is ideal for accommodating *nomadic* movement that works against striation; the fundamental antipathy between cybercriminals and gambling sites follows from their constitution of two incompatible kinds of space, smooth and striated respectively. As we will see, it is precisely when these two spaces come into contact that a cybercrime is committed; cybercriminals use smooth spaces to break striated spaces.

Smooth space is a space of wandering, "where the movement is more important than the arrival" (Bayne 2004, p. 303) and where "one's momentary location is less important than one's continuing movement... this space is by definition a structure for what does not yet exist" (Moulthrop 1994, p. 303). Nomads adhere to these smooth spaces and operate by "ascending and descending, emerging and receding" (Wray 2003, p. 5). This movement complements connectivity and multiplicity between different networked nodes that "distributes people... in an open space, one ... without division into shares, in a space without borders or enclosure" (Deleuze & Guattari 1987, p. 380). As Wray (2003) notes, rhizomatic links offer pathways through which nomadic movement occurs, thereby encouraging information flow in an open manner without external control. While this path is between two nodes, the trajectory in-between these nodes is

autonomous and has a direction of its own. Unlike striated space that treats the path as something between two predetermined points, smooth space gives priority to the path itself. Rhizomes comprise lines in motion as opposed to stationary points in striated structures. Rhizomatic nodes are relays along this trajectory, a *line of flight*, which continually resists the sedentary or the striated (Deleuze & Guattari 1987, p. 380; Genosko 2001, p. 1289). These flight lines are always "twirling, folding, unravelling and disaligning themselves" (Lort 2000, p. 1). Furthermore, these lines are different in each case, offering an available means of escape from control forces and taking nomads in any direction. But the speed of flight is not determined by their movement. As Deleuze and Guattari (1987) note, "a movement may be very fast, but that does not give it speed; a speed may be very slow, or even immobile, yet it is still speed. Movement is extensive; speed is intensive" (p. 381). It is important to note here that the nomad is not simply the byproduct of smooth space. Not only do nomads inhabit smooth space, but they also develop and extend it: "the nomad makes the desert [smooth space] no less than he is made by it" (Deleuze & Guattari 1987, p. 382). Nomads and smooth space work on each other; nomads add to smooth spaces by using a series of movements in varying directions, while smooth spaces foster nomadic movement. In the context of my research, I ask: How do techno-nomads (cybercriminals) move in smooth zones to break striated zones? How do cybercriminals use the rhizomatic properties of smooth zones to move? How do these rhizomatic traits impact the flight lines of cybercriminals?

Reconfiguring Community, Identity, and Territory

The development of this digital environment changes conventional notions of community, identity, and territory. Cyberspace generates numerous online communities with extensive memberships and interactions. Oldenburg (1989) suggests that individuals typically move through three environments where they work, live, and meet others. In contemporary societies, however, he says individuals experience only two environments (work and home), and when they feel abandoned and isolated, they turn more and more to the internet to experience bonding, belonging, and closeness. Rheingold (1993) and Jones (1995) claim that online communities have proliferated because of the excitement internet users experience when they interact with other people through new, digital mediums. They identify the unique traits of online relationships: the lack of face-to-face contact, the lack of spatial-temporal constraints, the use of computers for communication, and the ability to gain new information quickly. This notion of community seems apropos for recent forms of gambling. Since the mid 1990s, internet gambling has proliferated, offering an assortment of gambling sites, or communities, to its customers (CERT-LEXSI 2006, p. 3; BCPRG 2004, p. 1; Jepson 2000, p. 1). Gambling sites offer a variety of online services, such as lotteries, casino games, bingo, sports betting, and card games, where customers gamble and interact with each other (BCPRG 2004, p.1; Stewart 2006, p. 2). Each of these communities caters to different demographics and behaviours. Customers gamble for several reasons that range from relaxation and socializing with others to excitement and financial gain (Parke, Rigbye, Parke & Williams 2007; Tse, et al. 2005; Prus 2004). For instance, men often play for excitement, while women often play for relaxation (Parke, Rigbye, Parke & Williams 2007). Older people prefer

gambling activities that require less concentration and complex decision making, and prefer internet casinos over games like online poker (Griffiths 2006). Adolescents gamble for excitement and socializing with their peers (Meerkamper 2006). Thus, the online gambling community is attractive to an assortment of customers. Not surprisingly, specialized virtual communities, such as hacker communities, have also burgeoned, accommodating cybercriminal populations. In these communities, hackers interact through e-mails, bulletin-boards, and chat rooms. In addition to socializing, these venues may promote criminal tendencies, where hackers share information, learn from each other, or form alliances for future crimes. The uses of these communities as communication channels for hackers worldwide, and their importance in criminal activity, are discussed later.

Cyberspace also alters notions of identity, best captured by Baudrillard's (1988) concept of the hyperreal, where simulation stands in for the real, often replacing it. He claims that there is a blurring of the distinctions between the real and the unreal. With the evolution of technology, society becomes increasingly fragmented with freely flowing signs that have no relation to original referents. Cyberspace challenges notions of reality making much of the world virtual, where digital identities form and multiply. As Whitaker (1999) notes, individuals in cyberspace reinvent themselves in a "parallel world that may, or may not, ever converge with the 'real' world" (p. 56). M.U.Ds (Multi User Dungeons) and virtual communities offer playgrounds for the self. Here, environments of anonymity, distance, and flexibility allow individuals to test pluralistic ways of being that are alterable and open to interpretation, which, in turn, distorts the boundaries between real and simulated identities (Turkle 1997). Indeed, the anonymity feature of the internet

allows customers to privately participate in gambling without the fear of stigma and permits youth to use their parents' personal and financial information to create their own accounts with gambling sites, thereby generating simulated identities for themselves (Griffiths 2003, p. 559; SNJCI & AGNJ 2000). Identities in cyberspace, however, may be constituted outside the individual. Information stored in databases is combined to 'interpellate' numerous, fragmented, and decentered online identities without the subject's permission or awareness (Poster 1995). For instance, adolescents using their parents' information to gamble may result in several customer profiles unbeknownst to the parents. Gambling sites also store customer information, such as playing habits and favoured games to create customer-specific services, thereby externally interpellating the player. Though anonymity and multiple identities remove customer fears and offer secrecy, they create serious problems of accountability and the security of electronic information. For instance, a cybercriminal may create multiple identities, or multiple cybercriminals may use the same identity. This enables hackers to work individually or collectively to commit multiple crimes easily. Furthermore, tracing numerous identities back to its originating source becomes difficult; there are few reliable or easy ways to determine real identities on the web. Thus, hackers face little fear of detection, making cybercrime easy to commit, lucrative, and successful (McAfee 2007; Wall 2007).

Terrestrial conceptions of bordered space do not apply in cyberspace because the latter is comparable to a Deleuzian map that can be entered at any rhizomatic point at any time (Hamman 1996; Wray 2003; Wenninger 2007). Smooth territories lack an "external plan prior to the process of becoming, making or producing territories" (Wenninger 2007, p. 3). The dynamics of cyberspace, therefore, involve deterritorialization and

reterritorialization movements that are interconnected and occur simultaneously rather than in a sequential manner (Wenninger 2007). The movement of deterritorialization is inclined towards producing smoothness in a striated territory along numerous lines of flight, which, in turn, evokes the reterritorialization of that space. Deterritorialization produces "metamorphoses or creative ... mutations of the territories" (Wenninger 2007, p. 4). Furthermore, the dynamics triggering deterritorialization can also result from contact with other territories in cyberspace (Wenninger 2007, p. 4). One instance of deterritorialization can be seen in the work of hackers, the techno-nomads of cyberspace, who change closed territories (striated spaces), such as targeted gambling sites or databases. Hackers use multiple flight lines, or movements of *absolute deterritorialization*, which may include the use of viruses or cracking password-protected sites. This deterritorialization, in turn, evokes reterritorialization movements, such as the installation of security patches and firewalls, and governance structures for example, that generate new, reterritorialized website territories and databases, and new regulating environments (McMullan & Rege 2007). As Wenninger (2007) notes, reterritorialization is not a "process of coming back to the original territoriality"; it is a metamorphosis of the deterritorialized space through the "introduction of new arrangements of its parts or establishment of new relations between them or with other territories" (p. 6). These new territories are then modified by further deterritorializing movements, such as a hacker's development of newer viruses in response to security fixes. Morse (2006), Jepson (2000), and Stewart (2006) suggest that illicit gambling operations demonstrate their own deterritorialization movements by easily circumventing domestic regulatory systems, undercutting domestic tax structures, promoting money laundering schemes, and

inadequately protecting minors. Reterritorialization movements, such as international cooperation from law enforcers, security measures, and updated laws, respond to these unscrupulous gambling operations in cyberspace (Speer 2000; Council of Europe 2004; Kowalski 2002; Brenner 2001; Toscano 2000; Goodman 1997). As Deleuze and Guattari (1987) note, "one of the fundamental tasks of the State is to striate the space over which it reigns, or to utilize smooth spaces as a means of communication in the *service* of striated space" (p. 385). In other words, social control agents need to utilize the very smooth space inhabited by nomadic hackers to thwart cybercrimes and *reclaim* striated space through reterritorialization movements. For instance, techno-police may set up 'honey-pots', which are sites created by authorities to lure and trap cybercriminals. Here, law enforcement bodies employ the same tactics used by cybercriminals, such as anonymity and specialized digital techniques to "vanquish nomadism... [and] establish a zone of rights.. over all of the [information] flows" (Deleuze & Guattari 1987, p. 385). Several factors, however, may impede these reterritorialization attempts; the use of dummy IP (computer) addresses, suspect online identities, and anonymous re-mailer services by cybercriminals, along with fragile digital evidence, pre-digital police techniques, poor technological training, outdated laws, and complicated jurisdictional issues may collectively impact the successful detection, apprehension, and prosecution of hackers (McMullan & Rege 2007).

The concepts offered by Deleuze and Guattari (1987) are useful for theoretically conceptualizing the dynamics of cyberspace, the movements of techno-nomads (cybercriminals), the constant morphing of digital territories, and the formation of online communities and identities. But they cannot easily or obviously account for the detailed

ways that cybercriminals use these characteristics of cyberspace to organize and operate criminal activities. In order to add substance to the abovementioned form of my analytical framework, I include elements from the research on criminal organizations and organized crime that examine criminal typologies and factors determining their organizational dynamics. I then combine these theoretical bodies to create an integrated framework that allows me to account for online criminal organization, operation, and communication.

Criminal Organization and Organized Crime Theories

Many researchers have studied the organization of crime. Some studies have examined the organization of specific types of deviance, such as extortion, murder, and pickpocketing (Best & Luckenbill 1982; McIntosh 1975). Others have examined the relationships formed by specific deviants, such as racketeers, armed robbers, and thieves (Cressey 1969; Einstadter 1969). Still others have explored structural features, such as criminal roles, group dynamics, criminal expertise, and the characteristics of the offense and offender (Clinard & Quinney 1973; Gibbons 1977). For example, Cressey (1972) examined crime along the dimension of rationality. He argued that the greater the complexity (division of labour, coordination, and pursuit of shared goals) of the organization, the greater the rationality of crime production (Best & Luckenbill 1982). McIntosh (1975) also insisted that criminals organized themselves along rational lines. She argued that each type of crime was characterized by an organization that suited the nature of the activity, and was shaped by the context in which it operated. Unlike Cressey (1972), she stated that rationality was not sequential but context-specific, as the problems

posed by these contexts determined the appropriate organizational dynamics for criminal groups (McIntosh 1975, p. 17).

Other researchers have used cultural theory to study criminal organization arguing that cultures may be classified by rank and boundary, which designated and differentiated insiders and outsiders. Mars (2000) developed a fourfold typology of criminal organization. First, there were criminal individualists who had no ranking or boundary; they were entrepreneurs and opportunists who networked and competed. Then there were criminal isolates, who did not have a boundary but possessed a ranking system; they lacked group membership, and social and material resources, making them vulnerable to manipulation by the law and other criminals. Third, there were groups of organized criminals who had a clear ranking system and a degree of organizational stability. Insiders and outsiders were separated by a clear boundary. Finally, ideological criminals had a strong boundary but avoided any ranking system, promoting an egalitarian approach to crime. McAndrew (2000), however, argued that the concepts of rank and boundary were rather vague. He developed several mathematical concepts, such as *lines* and *paths*, to replace conventional concepts, such as *roles* and *criminal techniques*, to account for crime networks. Using mathematical combinations of lines and paths, McAndrew (2000) argued that crime networks could be tracked and studied with precision.

However, several problems are evident with this body of research. First, the research on the organization of deviance is often descriptive and does not offer a comprehensive theory of the organization of deviance or the organization of deviants. Cressey's (1972) typology, for example, does not account for the dynamics of

organizational change between rational crime groups. Second, the studies are either too narrow in scope, focusing on a particular form of crime, or too broad in scope, constructing general typologies of deviance or deviants. For example, McIntosh's (1975) classification provides the social organization of specific types of deviance, such as pickpocketing, robbery, and racketeering. This is problematic because my thesis explores online crimes, which may have radically different organizational dynamics. Mars' (2000) focus on rank and boundary is too narrow and does not capture other factors of criminal organization, such as goals, skills, subculture, and motivations. McAndrews' (2000) criminal network approach does not account for individual criminals or small crime groups, which are important to cybercrimes. Finally, the above-mentioned research often confuses two different foundations for analyzing organizations, namely criminal organization and the organization of criminal transactions. We need to distinguish between the patterns of social relations among criminal actors, and the patterns of social relations among the roles performed in criminal transactions, as these collectively determine the organizational dynamics of criminals and their activity. Theory should account for the causes, consequences, and social control of deviance and crime at an organizational level. These include the mechanisms by which criminals organize themselves to pursue their deviant goals, the difference in their organizational features (division of labour, coordination, and objectives), the organizational impacts, such as efficiency, success, and management of social control agents, the conditions that influence the organization of criminals, and the organizational changes over time.

Best and Luckenbill (1982) offer this intermediate level of analysis that dovetails with Deleuze and Guattari's (1987) rhizomatic approach and fits nicely with my research

project. They suggest that criminals organize themselves along three dimensions: (i) complexity – criminal organizations have a division of labour and members have different specialized skills, (ii) coordination – crime groups vary with regard to their roles and the rules their members follow, and (iii) purposiveness – criminal organizations vary with respect to their determination in achieving goals (Best & Luckenbill 1982, p. 24). The levels of complexity, coordination, and purposiveness, collectively determine the sophistication of criminal organizations, ranging from loners, colleagues, and peers to mobs and formal organizations.

Loners by definition do not associate with others. They operate on their own and develop personalized approaches to crime; a division of labour does not exist (Best & Luckenbill 1982, p. 24). Loners typically exploit specific circumstances: positions of trust, opportunity structures, special skills and knowledge, and the power to rationalize their illicit acts, which permit them to work by themselves. Avoiding detection, however, is often difficult because loners must juggle the tasks of committing crimes and serve as lookouts for their own misconduct (Best & Luckenbill 1982, p. 29). *Colleagues* associate with others but often commit deviant acts alone. They interact with each other to learn different criminal techniques, gain new knowledge, receive training, and obtain social support. Colleagues build their own shared knowledge base and subculture, which is transmitted through interaction. However, each individual determines his/her own success and collegial partners do not protect each other from failure (Best & Luckenbill 1982, p. 40). *Peers* cooperate with each other and commit criminal acts together. They execute complex tasks with ease and speed, which in turn allows them to avoid detection by law enforcement bodies (Best & Luckenbill 1982, p. 53). A minimal division of

labour exists, but no set hierarchy exists amongst peers. Nevertheless, peers have strong bonds; they provide social support and criminal equipment to each other (Best & Luckenbill 1982, p. 45). Like colleagues, peers have their own subcultures, where they learn criminal techniques and rationales for their criminal actions. Some peers, however, may have fleeting relationships with others, where they temporarily join forces to commit deviant acts, such as in stings or cons. After the crime these peers separate and their paths may seldom cross again until a new criminal project is formulated (Best & Luckenbill 1982, p. 47). Though peers remain companions for longer time periods and have group stability, they typically have limited resources (money, defense mechanisms) that protect them against external threats or social control agents, which may eventually cause organizational disintegration (Best & Luckenbill 1982, p. 53).

Mobs are small teams who regularly perform specialized roles in coordinating and conducting particular types of crime, such as theft (Best & Luckenbill 1982, p. 56). The mob's purpose is to make crime safe, successful, and profitable. Their organization is designed so that it is no larger than necessary, but large enough to ensure that the crime is executed efficiently and effectively (Best & Luckenbill 1982, p. 64). Mobs possess a fairly elaborate division of labour with each member specializing in a specific task. They have a subculture with their own vocabulary, a code of conduct for members, and a network of contacts with other criminals who assist the mob in the coordination of their criminal operations. Few individual members possess all the specialized skills needed to carry out crimes, and so a group of compatible criminals may work together for years often without any turnover (Best & Luckenbill 1982, p. 61). *Formal organizations* are the most sophisticated type of criminal organization. They exist primarily to acquire power

and money, and have large numbers of members who cooperate over "extended time and space" to commit crimes (Best & Luckenbill 1982, p. 65). Typically formal organizations have vertical command structures, horizontal divisions of responsibility, intimate family bonds, ethnic and kinship relations, and local territorial cultures and institutions (Abadinksy 1990; Lyman & Potter 1997; Cressey 1969; Ianni 1974; Reuter 1983).

But do mobs and formal organizations have to possess the structure and hierarchy implied in these models? Can you have organized crime that is formal but nevertheless exhibits minimal vertical striation in the ordering and execution of its activities? Chambliss (1978), Smith (1974), Albini (1971), and Lemeiux (2003) answer in the affirmative and stress the flexibility of formal organizations, which is especially apt for the world of cybercrime.

Chambliss (1978) argues that organized crime is often composed of an "overlapping series of crime networks with shifting memberships highly adaptive to the economic, political, and social exigencies of the community, without a centralized system of control" (p. 49). Decentralization of power is a major trait and so there is little vertical authority normally associated with formal organizations as evinced by Cressey (1969) and Best and Luckenbill (1982). Members are embedded in networks, some of whom are powerful enough to determine the activities of criminals. Connections between legitimate and illegitimate enterprises often exist and in many instances criminals may be more appropriately seen as "employees of the criminal network" (Chambliss 1978, p. 49). The crime group is comprised of several 'sub-networks' that work in a symbiotic fashion. Each sub-network is responsible for a particular task, such as accumulating capital,

recruiting, moving money, bribing officials, and enforcing violence, in order to ensure criminal success both locally and globally.

The Enterprise Model, as evinced by Smith (1974), holds that criminal groups are primarily conditioned by the principles of supply and demand. According to him, the illegal market is an extension of the legal economy. The demands for illegal goods and services, such as drugs, loansharking and smuggling are not met by the legal market, and so organized crime groups fill this market vacuum. They operate with the "same fundamental assumptions that govern entrepreneurship in the legitimate marketplace" and the underground economy is structured like the legal economy (Lyman & Potter 1997, p. 48; Smith 1974). But there is little centralization of authority or power because illegal enterprises consist of numerous, fragmented, opportunistic criminal groups (Lyman & Potter 1997, p. 48). Economic considerations, not hierarchical or ethnic considerations, form the basis of membership and organization. Not surprisingly, illegal businesses have special groups for handling their commerce: purchasers who buy illegal products from their sources, sellers who market illegal products to consumers, and enforcers who collect payments from uncooperative customers, manage competition, and discipline problems within the criminal organization itself. Just like licit enterprises, the greatest foes of illegitimate enterprises are their competitors. Competition must be discouraged. But unlike legal governance in the legitimate world of capital, control is accomplished through employing violence, corruption, and extortion in order to expand markets and increase profits (Lyman & Potter 1997, p. 77).

Albini (1971) views organized crime as a series of specific patron-client relationships. Organized crime groups "resemble a system where whoever has the most

power is able to render the greatest services [and] control support" (Hagan 1994, p. 469) The structure is based on a developmental-association system of "peer relations, that are informal, flexible, and constantly immersed in conflict" (Hagan 1994, p. 469). Power relationships are decentered and are constantly being formed, dissolved, and re-formed with new actors (Lyman & Potter 1997, p. 47; Albini 1971). The organizational qualities of crime groups are loose structuring and adaptability which, in turn, provide contacts, assist recruitment, and help coordinate the "specialized talents and services necessary for criminal entrepreneurship" (Lyman & Potter 1997, p. 48). Members are occasionally or loosely affiliated only coming together in pursuit of particular sources of profit on a project by project basis. Flexibility ensures organizational persistence and stability because when a "powerful syndicate figure is incarcerated, all that has really been severed is his position as a patron to his clients" (Abadinsky 1990, p. 26). Replacements are easily recruited, and the network continues to operate because it is eminently adaptable to change. Criminal group interest and solidarity is attained through cooperation and accommodation, and violence is employed only as a last resort.

Lemieux (2003) brings together many of the ideas developed by Albini (1971), Smith (1974), and Chambliss (1978) into what he identifies as the nine roles inherent in most criminal networks of any size. At the core of a criminal network are the *organizers*, who determine the nature and scope of activities. They also offer the guidance and impetus necessary to carry out these activities (Lemieux 2003, p. 12). The *executors* are responsible for carrying out the objectives of the organizers. They implement the attacks according to the plans laid out by the organizers, and they may even possess the specialized skills necessary to successfully carry out the operation, such as malware

development and hacking expertise. There are also *money movers* who collect money from the victims and return it back to their criminal enterprise. The money movers are also responsible for channeling funds through several paths in order to mask or distort the paper trail. Then, *insulators* work to protect the internal structure, the core, from being exposed. They channel orders or guidance from the center of the network to its periphery. They also guarantee the proper flow of communication between the sub-networks without revealing the core (Lemieux 2003, p. 12). The *communicators* handle the effective flow of information between the various sub-networks. They gather feedback regarding orders that are transmitted to other actors in the network. There may be tension between insulators and communicators, as their roles may clash (Lemieux 2003, p. 13). To avoid this conflict, an individual may sometimes simultaneously take on both roles. *Guardians* are the protectors of the criminal network and they take the measures necessary to prevent external attacks. Unlike insulators who protect the criminal core, guardians protect the entire network from exterior threats. They determine the loyalty of newly hired recruits, and detect spies, informers, or infiltrators in the criminal network. Guardians seek to "prevent defections from the network actors and to minimize damages when defections occur" (Lemieux 2003, p. 13). The *extenders* are responsible for the expansion of the criminal network. They recruit new members, negotiate with other sub-networks, manage competition, and encourage collaboration with other illegal businesses, government and justice agencies. Several tactics are deployed, ranging from "voluntary recruitment through bribery and corruption to involuntary recruitment through coercion", supported by incentives or violence (Lemieux 2003, p. 13). *Monitors* deal with the effectiveness of the network. Their responsibilities include "providing information to

organizers regarding weaknesses and problems within the network so that the organizers can resolve them" (Lemieux 2003, p. 13). Monitors also ensure that the network can adjust to different circumstances and aid in developing techniques to circumvent law enforcement (Lemieux 2003, p. 13). Finally, there are *crossovers* who are part of the criminal network but also belong to legitimate governmental, financial or commercial sectors. As such, crossovers provide invaluable insider information, thereby contributing to the effectiveness of the organization from within, and protection of the network from outside attacks (Lemieux 2003, p. 13).

There are several advantages arising from this networked structure in regard to criminal events. First, there is no head authority in control; sub-networks have the freedom to operate autonomously. Second, the loose connections within the network allow for flexibility, which facilitates the "rapid reorganization of criminal activities in response to changing consumer demand and law enforcement activities" (Schloenhardt 1999, p. 13). Not surprisingly, these networks are sometimes described as "disorganized", and it is precisely this quality that makes them dynamic and efficient: "if a node or hub disappears, nodes may simply move their connections to others", thereby exhibiting regenerative tendencies (Yoo 2005, p. 2). Finally, the network model is less vulnerable to social control. Only smaller units are exposed to policing agents, leaving the rest of the network intact: "free-scale networks remain remarkably immune to attack; randomly destroying nodes will not cause [the entire network] to collapse" (Yoo 2005, p. 2).

Cyberspace creates new opportunities for criminal organization, operation, and communication. The organizational dynamics of criminals change in this digital environment (Wall 2007; Brenner 2002). The abovementioned theories of criminal

organization and organized crime help identify and extract important dimensions of the organization of criminals, such as scope, size, life cycle, associations and partnerships, division of labour, and management of external threats. They do not, however, account for how these dimensions are impacted by digital environments and how these, in turn, influence online criminal organization and cybercrimes. I therefore propose an integrated theoretical framework to account for the organization of cybercriminals, their crimes, and communication.

Integrating Rhizomatic and Criminal Organizational Theories

I draw from Best and Luckenbill's (1982) typology to account for small-scale cybercriminal organizations, such as hacking and player collusion, and I employ Chambliss' (1978), Smith's (1974), Albini's (1971), and Lemieux's (2003) formulations to help explain more complex criminal organization, such as cyberextortion and money laundering. I combine these organizational typologies with Deleuze and Guattari's (1987) theory of rhizomes, smooth and striated spaces, and deterritorialization and reterritorialization movements, which allows me to address the questions raised in this chapter and to examine how nomadic cybercriminals inhabit and move in the smooth spaces of the web, break striated spaces through deterritorialization movements to develop and extend smooth spaces, and organize themselves to commit crimes successfully and efficiently in cyberspace. I now present six points of intersection of rhizomatic theory and criminal organization, focusing on their implications for the organization, operation, and communication of criminal events.

Space, Site, and Scope of Crime

Nodes in digital smooth spaces can connect with each other in any sequence and can be located anywhere in the rhizomatic internet. Together, the principles of connectivity and cartography facilitate the linking of nodes worldwide in infinite combinations, which, in turn, transcends geographical conceptions of location and space. Cybercriminals all over the world now enter digital environments from any port and can form alliances in any combination. Furthermore, this sequencing may or may not be predetermined depending on the nature of criminal activity; cybercriminals can connect with each other dynamically to create diverse organizations that are both small and large in membership and sophistication. Unlike mobs that operate at specific geographical sites, connectivity and cartography provide significant organizational flexibility to *digital associates* and *striated assemblages* (online organized crime groups) allowing them to extend the scope of their memberships, partnerships, and activities.

Nodes can also account for sites of victimization and victims (gambling sites, gaming software, honest players) as well as sites of perpetration and perpetrators (gambling sites, hackers). A cybercrime can be committed at any node from any node in cyberspace, making the connections between these nodes "glocalized" (Wall 2007, p. 38). Here, criminal processes are not *trans*national in scope; traditional geographies collapse and there are intrinsic linkages between global and local sites. A cybercrime (disseminating virus) committed at a local node can have impacts on several global nodes (websites, PCs), and vice versa, such as dispersed computer systems attacking a gambling site (local node). This extends the reach of criminals across jurisdictions, thereby offering increased scope and flexibility when compared to offline criminal activities of peers and

mobs, whose crimes are geographically restricted. The internet also transforms the power placed in the hands of loners and colleagues. This results in the "empowered single or small agent" (as cited in Wall 2007, p. 39). Unlike the conventional loner or colleague portrayed by Best and Luckenbill (1982), *techno-nomads* can now commit crimes that were previously beyond their financial, organizational, and spatial abilities (Wall 2007, p. 40). Online crimes can spread across a broad geographical space and can be committed with inexpensive technology that is easily available. Crimes that once required planning and coordination can now be committed by a single individual. Techno-nomads may exploit networked systems to repeatedly execute complex crimes alone with greater ease and efficiency. The organizational flexibility afforded to cybercriminals allows them to form multiple alliances in order to commit numerous cybercrimes. Nodes can also account for different computer systems, such as databases, servers, networks, and mainframes, which are the targets of cybercrimes. The rhizomatic digital space connects several computer systems in different sequences, which allows cybercriminals to connect to and attack targets either directly, or indirectly through other networked systems. Additionally, cybercriminals can attack the same target through different sets of connections. This endless permutation of linkages gives cybercriminals greater flexibility; using unpredictable sequences to target any node make locating their site difficult.

Finally, the ability to connect from and to anywhere in any way in the rhizomatic digital space also helps cybercriminals network with each other. For instance, the use of bulletin boards and chatrooms can help extenders in striated assemblages to recruit new executors for criminal activity. These extenders can be located at any node in the digital

environment and can reach potential recruits at glocalized nodes. Furthermore, online hacking communities can be created around specific interests, where hackers from all over the world can upload and download the latest viruses, and disseminate information regarding attack techniques, vulnerable targets, and references to hackers-for-hire, which permits techno-nomads to easily access information, and digital associates to form alliances that surpass geographical boundaries. Thus the scope of interaction, partnerships, and information exchange radically increases because of digital environments and technology.

Time, Transience, and Criminal Life-Span

The principles of connectivity and cartography also alter the membership of criminal organizations. Criminals can connect from and to any node in the networked digital environment at any time. As such, criminals can come together for a limited period of time to commit specific crimes and depart upon their successful completion (Brenner 2002). This challenges conventional notions of criminal organizations, such as peers, mobs, and formal organizations, that must exist for long periods of time with little turnover to be successful. By engaging in ephemeral partnerships, members of *digital associates* and *striated assemblages* do not commit to any specific criminal organization, thereby giving them greater flexibility in their activities. This fleeting membership, in turn, makes the criminal organization transient in nature; its life-span is determined by the duration of its criminal activity. Additionally, smooth space permits regeneration, where new paths are created to take over disrupted paths. If a particular criminal node is detected or compromised, the criminal organization connects to another sequence of

cybercriminals to continue its operation, making its existence persistent (McMullan & Rege 2007).

Cyberspace and ICTs allow cybercrimes to be committed either "synchronously in real time, or asynchronously in chosen-time" (as cited in Wall 2007, p. 39). Crimes that were traditionally limited by temporal factors can now be executed at the cybercriminal's will and needs. Furthermore, the criminal activity itself can have a fluctuating duration. Cybercrimes can be carried out continuously and intensely for a short time, or intermittently for a longer time frame, or some combination of both. Moreover, assemblages of computer connections in digital environments permit cybercriminals to direct these crimes at multiple targets concurrently. Thus, conventional notions of time collapse in cyberspace; time is a flexible entity that can be manipulated by cybercriminals.

Communication and interaction between cybercriminals is also benefited by this pliability of time. ICTs speed the flow of information exchange between criminals. They can meet in chat rooms and communities in real-time to swap skill sets, criminal tactics, and/or contact information. Cybercriminals can also engage in email exchanges to plan and coordinate activities in their own chosen-time. Furthermore, information availability can also have fluctuating durations; some websites, such as hacker communities, can exist for extended time periods, while other websites, such as underground networks, can be dissolved upon the threat of exposure, or crime completion.

Lateral Assemblages, Horizontal Striations, and Crime Networks

Smooth cyberspace is a rhizomatic assemblage of networked nodes. Cybercriminals who work together in ephemeral memberships create networked organizations that have no set structure or hierarchy. Unlike Best and Luckenbill's (1982) conceptualization of formal organizations, online criminal networks use less hierarchical structures than traditional gangs (McAfee 2006, p. 4). These striated assemblages exhibit the decalcomanic principles of the digital environment in which they operate; they are decentered and lateral (Brenner 2002). The principles of connectivity, cartography, and multiplicity permit cybercriminals to connect to and from anywhere in numerous ways, which gives them a relatively disorganized organizational characteristic. Here, the term disorganized implies the lack of a fixed structure. Unlike traditional criminal organizations that involve face-to-face contact between members, online crime groups have members that are scattered worldwide and never meet in person, which makes cybercrime faster and more flexible than terrestrial organized crime (McAfee 2006, p. 4). Criminal organization involves several nodal clusters (groups of cybercriminals) that specialize in specific skills, such as malware production, decryption programs, and hacking. While this organization may be flat with a horizontal division of responsibility, nodal clusters themselves may exhibit some striation. Each cluster has its own organizer, who coordinates and plans the nodal activity. Thus, the organization of these *striated assemblages* is flat and may exhibit minimal hierarchy, when compared to Best and Luckenbill's (1982) hierarchical mobs and formal organizations.

Cybercrime also operates as an assemblage of attack methods. For instance, cybercriminals converge and interconnect different criminal techniques, such as email

spams and viruses, thereby creating networked attacks. The principles of connectivity and multiplicity allow cybercriminals to target their victims along different dimensions. Here, attacks themselves can be structured as nodal assemblages. For instance, hackers may use viruses to remotely control numerous nodes (computers, servers, databases) in cyberspace. They may then draw these compromised machines together to form a disorganized assemblage or army to attack their targets. In this context, the remotely controlled machine (operated by techno-nomads, digital associates, or striated assemblages) is in a position of striation as it orders its army of compromised machines to attack specific targets.

The principle of decalcomania also affects the communication channels used by cybercriminals. First, there is an increasing convergence and interfunctionality of computing technologies in cyberspace, enabling cybercriminals to construct new communication assemblages, such as peer-to-peer networks, grid technologies, and networked databases that permit decentralized information flow and exchange (Wall 2007, p. 36). Second, communication assemblages can also be created by the combination of different networking nodes, such as email, hacking websites, blogs, chat rooms, and bulletin boards. The principles of connectivity and multiplicity contribute to this rhizomatic communication. Networking mediums can be used in any sequence and in numerous ways, which gives this communication assemblage flexibility; the "viral" or "rhizomatic" information flow contributes to the circulation of criminal ideas, thereby facilitating the communication and interaction of cybercriminals. Furthermore, the ability to link these channels together in dynamic, unpredictable, and countless ways makes detecting the communication mediums of cybercriminals difficult to discover and track.

Flows, Flight Lines, and Criminal Events

The rhizomatic space in which cybercriminals operate is a dynamic space, which promotes fluid movement. The principle of multiplicity, as noted earlier, allows cybercriminals to link together along several paths, which can involve direct or indirect connections between nodes scattered in smooth space. The disorganized assemblage of cyberspace involves several networked nodes that serve as origins or destinations of different flight lines. Cybercriminals use these trajectories to travel sporadically, which makes their location and structure often unpredictable and unknown. First, criminal organization becomes flexible as cybercriminals can unite from anywhere along numerous trajectories. Second, the choice of specific paths is not predetermined; a link between two nodes does not exist until the cybercriminal chooses to do so. Also, cybercriminals can use this feature to engage in a high turnover of movement when they are exposed, enabling them to mask their trail. Third, cybercriminals can remain anonymous as tracing the attack along multiple paths often misleads social control agents. Techno-nomads work along several remote flight lines in digital environments and so, unlike loners and colleagues who are more susceptible to exposure, techno-nomads can operate with little fear of discovery.

The principle of multiplicity also impacts criminal activity. Multiple paths offer an assortment of trajectories (flight lines) to cybercriminals along which they can engage in different criminal tactics (deterritorialization movements); hackers can victimize their targets through several avenues. For instance, one attack can involve "hopping" through servers located in a certain set of countries; subsequent attacks may involve servers in entirely different countries. Thus, cybercriminals avoid creating attack patterns or 'digital

signatures' as rhizomatic environments give them greater flexibility. This makes tracing the source and nature of the attack difficult.

Interaction between cybercriminals is further facilitated by the fluidity of cyberspace. Hackers can connect to various communication channels through multiple paths. The interplay between connectivity and multiplicity enables cybercriminals to correspond with each other via different connection sequences that result in multiple and fluid paths of information exchange. Furthermore, these covert communication channels can remain protected and unidentified through a series of pathways that layer its location. Thus, these flexibility and covert networking opportunities facilitate cybercriminal interaction.

Zones, Deterritorialization, and Criminal Techniques

The rhizomatic principles of connectivity, heterogeneity, and cartography are key in determining the features of criminal organization. These characteristics transform criminal organization allowing a "new genre of collaborations between different offending groups: hackers, virus writers and spammers" (Wall 2007, p. 40). This marriage of skills allows divisions of labour to become highly specialized, as an array of expert individuals can be drawn together with ease in the cyberspace assemblage. As Wall (2007) notes, the "higher specifications of sophisticated malicious software today require increasingly specialist skills in their construction" (p. 41). Furthermore, cybercriminals can connect with each other in any number of combinations, resulting in a variety of organizations that can overlap. Cybercriminals benefit from these characteristics as they can organize themselves with greater flexibility and efficiency.

Also, hackers can organize around common goals and motivations, such as curiosity, thrill, challenge, and profit.

The act of cybercrime involves gaining access to closed/striated zones, such as secure gambling sites, firewall protected servers, and password-protected databases. The principle of multiplicity is useful as it allows cybercriminals to conduct crimes through various pathways. These paths serve as lines of flight, which are movements of absolute deterritorialization. Techno-nomads, digital associates, and striated assemblages deterritorialize (hack, crack, decrypt) striated zones in cyberspace along these multiple trajectories. Their deterritorialization movements vary depending on targets, alliances, disruptions, and obstacles, resulting in diverse technological attacks that are often context-specific. Furthermore, the property of heterogeneity permits cybercriminals to attack different striated spaces in the digital assemblage. The deterritorialization movements of cybercriminals impact cyberspace by altering its smooth and striated zones. Striated spaces, such as protected servers, are broken or hacked to create smooth spaces, such as infecting these servers with viruses in order to control them. These smooth spaces, in turn, harbour the nomadic movement of cybercriminals, who can use smooth spaces to create new lines of flight, for example, by using the compromised machines to attack other targets.

Cybercriminals can have both smooth and striated zones of communication. For instance, cybercriminals can visit and interact in public forums, such as bulletin-boards and blogs, where they can exchange information, seek support, or subscribe to a common hacker subculture. Alternatively, cybercriminals can have protected communication channels, such as private hacker communities that require password-protected user

accounts, or e-mails, which are preferred for covert communication when planning, coordinating, and executing specific attacks. Furthermore, cybercriminals can also use combinations of smooth and striated zones to make communication for their activities flexible and clandestine. For instance, striated assemblages may use public newsgroups to hire hackers for specific projects and then use private communication, such as e-mails to disseminate attack instructions. Finally, cybercriminals can also intercept the communication mediums of state and security agents by using specific deterritorialization movements. Cybercriminals can, for instance, use several decryption programs to decode underground reterritorialization movements, such as the latest honeypots, infiltrations, and apprehensions.

Managing Reterritorialization, Governance, and Security

Cybercriminals manage reterritorialization using the principle of regeneration. If police or security agents detect or disturb (reterritorialization) the movement of cybercriminals, they can create new lines of flight around these disruptions. The rhizomatic assemblage of cyberspace and the speed of ICTs allow cybercriminals to regroup along new flight lines with ease and efficiency. Cybercriminals can also manage reterritorialization movements by forming alliances with members within reterritorialization agencies. For instance, crossovers can offer insider information on forthcoming reterritorialization movements, which permits cybercriminals to dissolve any partnerships and form new alliances with different members. Thus, the use of insiders and dynamic organization permits cybercriminals to successfully manage reterritorialization.

Threats of reterritorialization to criminal activity can be managed in two ways. First, cybercrime can be persistent by using the principle of regeneration. If a node that handles a specific criminal task is detected/disrupted, cybercriminals can move the entire operation to different nodes via multiple flight lines. Individual hackers can also resist reterritorialization by abandoning detected trajectories and using new flight lines to resume their activities. A second way to respond to reterritorialization is to use revised deterritorialization movements. Cybercriminals can use modified criminal techniques to recapture spaces taken over by reterritorialization agents; hackers may develop more sophisticated attacks that policing and security agents are unfamiliar with, thereby allowing cybercriminals to continue their criminal activities.

Covert interaction channels discovered by reterritorialization agents can be shut down, only to surface elsewhere in the networked assemblage, thereby maintaining communication in criminal groups. Communication nodes are disposable and can be generated sporadically at the hacker's will with ease. Cybercriminals benefit from the principles of connectivity, heterogeneity, and regeneration to create different communication channels using an assortment of nodes, which offers them flexibility and keeps their communication clandestine from reterritorializing agents.

Indeed, cyberspace radically transforms criminal activity and the anatomy of criminal organization and communication. As Wall (2007) and Brenner (2002) note, these criminal organizations are unique and depart from traditional ways of thinking about organization, operation, and interaction. The networked structure of cyberspace provides a new conduit for criminal activity, widening the perpetrator's reach of opportunity across jurisdictions, allowing wide-spread victimization, and providing new

avenues for organization and communication. By combining cyberspace theories and criminal organization theories, I demonstrate how digital environments affect criminal organization, operation, and communication. The above-mentioned dimensions can work in isolation, but more likely occur together, creating numerous possibilities for cybercrimes and cybercriminals. I use this integration to propose three types of online criminal organization: (i) individual *techno-nomads* who may or may not interact with other techno-nomads, operate alone, have a wider scope, and a longer life span, unlike Best and Luckenbill's (1982) loner, (ii) *digital associates* that are small-scale organizations comprising two or more members, have a simple division of labour, and extend over space and time, which also departs from Best and Luckenbill's (1982) peer, and (iii) *striated assemblages* who follow Lemieux's (2003) sophisticated networked criminal groups, but still exhibit some hierarchy and control. I use this framework to analyze my data in order to explore criminal organization, operation, and communication in the context of gambling sites.

Conclusion

This chapter addresses postmodern theories, criminal organization theories, and organized crime models, which I combine to create an integrated framework that allows me to study the organizational dynamics of cybercrimes and cybercriminals. In light of this integrated framework, I ask: How do techno-nomads, digital associates, and striated assemblages operate at gambling sites? How do they use rhizomatic principles to organize and operate in different contexts (hacking, collusion, cyberextortion)? Are certain cybercrimes committed by specific types of online criminal organizations, and if so, what deterritorialization movements are specific to each type? Do these types cross

paths, interact, and/or conflict? How do these types impact the smooth and striated zones in which they operate, and how do these spaces, in turn, determine each type's movement? Are these fluid and flexible organizations vulnerable to reterritorialization? If so, how does each type respond to these threats?

In order to address these questions, I collect information on the numerous types of cybercrimes occurring at gambling sites, namely hacking, cyberextortion, money laundering, player collusion, fraud, and the promotion of underage gambling. I conduct a document analysis of the existing secondary literature, unearth many relevant articles and case studies from newspapers, magazines and journals, and gambling and government websites, and formal legal, policing, and security reports. The next chapter, methodology, explains the nature of my data, and shows how I utilize it for analytical purposes.

Chapter 3

Research Methods

Introduction

The methodology I use in this research is document analysis, especially of company reports, government statutes and inquiries, financial reports, gambling commission reports, academic texts, journal articles, newspaper and magazine articles, legal cases, security archives, technical white papers, gaming developers' papers, and "how-to-do-it" hacker manuals. For the most part, I use text-based documents as 'cognitive maps' to chart out criminal techniques, social networks, and social practices surrounding cybercrime and its control (Mason 2002, p. 71). In this chapter, I define and explain why I use document analysis in my research. Next, I present my methodology and outline my data collection, sampling, and coding processes. Then I discuss the methodological limitations of my thesis, and how they are addressed. Finally, I conclude by describing the implications that my methodology has for my research project.

Document Analysis

Document analysis involves gathering and analyzing the content of texts. The content is any message that is communicated, while the text is that which serves as a medium for communication. Document analysis "lets a researcher reveal the content (i.e., messages, meanings, etc) in a source of communication (i.e., a book, article, movie, etc)" and permits content comparisons across many texts (Neuman 2003, p. 311). This method is useful for three types of research problems; those (i) with large volumes of text, (ii) with topics that must be analyzed from a distance, and (iii) with messages in texts that are otherwise difficult to obtain through casual observation (Neuman 2003, p. 311).

Document analysis is an appropriate research method for my thesis for several reasons. First, data on the phenomena of cybercrime and online gambling is not easily available through other methods. Finding cybercriminals to interview or survey is nearly impossible because they belong to an underground culture that is unknown or inaccessible. Similarly, observing hacker chatrooms and other communication channels where cybercriminals interact is difficult because the mediums they use are dynamic and secretive. For example, if cybercriminals detect anomalies in their communication traffic, or sense exposure, they can shut down their channels and reopen them elsewhere, making them difficult to track for research. Second, even if the communication medium is determined, acquiring access to online deviant interaction requires technical expertise and covert observation, which are beyond my technical abilities and raise ethical issues. Covertly observing online activities may be a potential invasion of privacy, and using excerpts of logs and chat room transcripts for research without the informed consent of participants, may create tension and mistrust if participants discover that their intimate or valuable conversations form the basis for social science research. Third, interviewing law enforcement personnel and gambling industry representatives is equally challenging. The former are often hesitant to disclose confidential case information, which may include up to date counter strategies, digital evidence and equipment, and the implementation of social control efforts. Most gambling industry representatives are reluctant to disclose cases of fraud, theft, and extortion for two reasons: (i) website operators fear that they are perceived as either vulnerable to attack or willing to pay ransoms, which, in turn, encourages further attacks, and (ii) public knowledge of victimization creates market credibility issues, and drives customers away from established services, thereby

benefiting competitors. Finally, the borderless nature of cybercrime and the speed at which it occurs, make observational methods difficult to apply, especially when the crime is in progress. Observational techniques are also difficult given that cyberspace is dynamic and offers anonymity to its users, which is problematic on two fronts. First, ambiguity arises when determining *who* or *what* to observe. For instance, observing hackers, organized cyberextortion rings, or cheaters, in action is difficult because they often utilize (i) multiple identities to remain anonymous, thus remaining hidden from researchers and (ii) specialized tactics that are beyond the technical know-how of sociological researchers, who may not realize that a cybercrime is transpiring. Second, determining *where* to observe is very challenging. Cybercrime is global in scope; perpetrators and victims are scattered worldwide. For example, identifying the online communication channels used by cybercriminals is difficult as these are poorly documented or altered in police documents and security reports. Also, observing gambling sites committing cybercrime is difficult for two reasons: (i) detecting cheating or other anomalies in the play requires researchers to be expert gamblers (AbsolutePoker.com), and (ii) some fraudulent sites have short life-spans as they shut down upon the completion of their crimes, or when they fear exposure (UKnlotteries.com, mass-lottery.org).

The problems in the above-mentioned research methods arise due to the paucity of prior research in this area. Earlier work offers little with respect to cybercrimes at gambling sites, how and where cybercriminals communicate, the origins and types of attacks, and the organizational characteristics of cybercriminals. As such, learning and building from earlier research, and employing their research methods to study my area of

interest, is problematic. So, conducting preliminary research is necessary to open up the phenomenon of cybercrimes at gambling sites.

Document analysis fits nicely with the exploratory nature of my research. First, as Dantzker and Hunter (2006) note, documents assist in discovering "why or how an event occurred and whether such an event could happen again" (p. 74). Indeed, documents allow me to examine cybercriminals, online crimes, and their properties. In addition, this method involves the analysis of preexisting data in a different way so as to answer different research questions than originally intended. Regardless of the context and content of earlier documents, I can reorganize and analyze them to specifically address my research objectives. A second reason for using this method is that documents provide a way of gaining access to events or processes, which you cannot observe "because they have already occurred, [or] because they take place in private" (Mason 2002, p. 73). In the context of cybercrime at gambling sites, documents can 'unlock' the otherwise covert elements of online criminal organization and operation. They provide information which is otherwise untraceable, such as the scope, origin, characteristics, and technical methods of digital attacks (PolicyHub 2007, p. 7). Third, documents permit an "alternative angle" or add "another dimension" to the research process because they allow for detailed pictures of social phenomena to emerge (Mason 2002, p. 109). For instance, a combination of newspaper articles, academic studies, and government reports generate a dialog between these information sources, thereby providing a well-rounded understanding of cybercrimes at gambling sites. Document analysis permits me to triangulate different sources in order to get a plausible picture of the phenomenon under study, and track it over set periods of time. A fourth reason for using this method is that a

variety of documents on cybercrime at gambling sites are already available and easily accessible (Berg 2001, p. 258). Information can be gathered through library and internet research [see next section] and the global reach of the internet permits me to access the latest worldwide information on my topic, thereby widening the scope of my document base. Finally, documents are non-reactive; researchers do not impact the situation (i.e., bias participants) as they may when conducting interviews of observations. For instance, questioning gambling industry representatives about the adequacy of their security measures may provoke incorrect or misleading responses, as a result of pleasing the researcher or avoiding embarrassment. With document analysis, the data collection process itself does not impact the content of preexisting data; researchers do not intrude on what is being studied, and thus cannot affect the outcomes of earlier research. Furthermore, this method enables researchers to obtain data without being present in the field. This addresses the problem of examining the borderless and speedy nature of cybercrimes. Additionally, the researcher can gain data via unobtrusive tactics thereby addressing the above-mentioned ethical problems. All these factors make document analysis ideal for my exploratory study. The systematic use of this method aids with identifying and connecting crucial concepts during data collection and coding, as discussed next.

Data Collection

The internet is a global medium that speeds the flow of information internationally, providing an abundance of documents from all over the world. It is being used more frequently in social science, as researchers realize that technology is broadening their research possibilities. Computer-mediated communications (CMCs) reduce the costs of traditional research methods and offer "interpretive flexibility" with the passage of time (Mann & Stewart 2004, p.367; Paccagnella 1997, p.2). The internet has 'links' that instantly connects individuals to multiple sources of information, thereby providing access to cross-referenced material (Neuman 2003, p. 114). These benefits permit researchers to study areas such as the hacking of satellite services, telemarketing fraud, pornography, and software piracy (Mann & Sutton, 1998; Shover, Coffey & Hobbs 2003; Taylor, Holland & Quayle 2001; Goodson, McCormick & Evans 2001); the web, however, has received little attention from researchers interested in studying criminal activity at gambling sites (McMullan & Rege 2007).

The internet housed an assortment of relevant resources and was used as a systematic research tool in this study. News sites (MacNewsWorld, Las Vegas Business Press, and Sun-Sentinel) offered the latest media accounts of internet gambling prevalence, gambling technology, gambling crime, as well as the manipulation of customer information and gaming software. Financial websites, such as Financial Action Task Force (FATF), Financial Crimes Enforcement Network (FinCEN), provided data on organized crime, money laundering, and internet gambling. White papers published by general security firms (McAfee, Symantec, Norton) offered information on organized cybercrimes, exploitation of system flaws, and the problems of legal governance. Reports

published by gambling commissions (Alderney Gambling Control Commission) exposed and explained the vulnerabilities of online gambling, policy and regulatory issues. Online gambling magazines provided information on specific cases of fraud, such as Starnet, MaxLotto, and Absolute Poker, as well as cases of gambling site victimization, such as CryptoLogic, Inc. Reports from specialized security sites (Prolexic, DigiDefense) revealed security measures for gambling sites, such as protection services against denial of service attacks, 'intelligent net-based' systems that detected anomalies in website traffic, and specialized techniques that thwarted attacks. Game developers associations, such as the International Game Developers Association (IGDA), provided online reports on software manipulation, attack typologies, and prevention techniques. Special interest websites, such as hacking and technology sites offered cybercriminal interviews, motivations, techniques, and information exchange between hackers. Journal articles on the internet offered information on how players worked together to cheat gaming systems at betting sites. Reports published by government agencies, such as the General Accounting Office (GAO), Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and FinCEN, examined how cybercriminals used gambling sites as mediums to commit their crimes. These reports, for example, provided information on how organized crime groups abused the payment mechanisms offered by gambling sites to launder their funds. Finally, law enforcement websites offered formal reports on cybercrime cases. They outlined the detection and apprehension of cybercriminals, and provided overviews of several sting operations.

I used the Google and the Google Scholar search engines to retrieve these internet articles for my research because they were the largest search engines on the web and

offered four advantages. First, they coded more pages and created the largest index possible for my detailed research. Google indexed web pages (.html files) as well as 12 other file types, such as PDFs, Word Documents, Excel Spreadsheets, Powerpoints, and plain text files, which enhanced the reach of information available. Google crossed language barriers via its WebPage Translation technology, which allowed me to access more materials in languages other than English. Second, Google 'crawled' the Web using two bots (software) at varying depths and times. The 'deep crawl bot' operated about once a month, adding fresh websites, dropping expired ones, and (re)creating an updated index of websites. To stay current Google also used 'fresh crawl bots' that performed a more cursory and frequent browse of the internet (Hill 2004, p. 1). These fresh crawl bots visited pages that were already in the Google index, "picking up new pages along the way" (Craven 2007, p. 1). These new pages were inserted into search results instantly, enabling me to find them immediately. The combination of these two crawls presented me with the latest data, which was useful to explore the dynamic phenomenon of cybercrimes at gambling sites. Third, Google provided "PageRank" technology, which was a numeric value that represented the importance of a website. Most search engines ranked pages by how frequently the search terms occurred in the returned page, or how strongly associated the search terms were within each resulting page. The PageRank algorithm, however, relied on the networked structure of webpages to determine a page's value. Google used a "democratic system", where it interpreted a "link from page A to page B, as a vote by page A for page B" and also analyzed the weight of the page casting the votes to determine its relevance (GoogleTech 2008, p. 1). It combined this technology with sophisticated text-matching methods to deliver pages that were important to my

keyword searches, from which I retrieved *relevant* research documents and webpages (GoogleTech 2008, p1). Finally, I used the Google Scholar search engine which indexed scholarly literature across disciplines and publishing formats. The Scholar index included many peer-reviewed online journals and websites. It allowed me to search for digital copies of articles both online and in libraries. Its 'cited by' feature listed other articles that cited the articles currently being viewed and the 'related articles' feature listed related articles in relevance to the original search results. Both these features linked me to a pool of relevant articles that I otherwise may not have obtained, which further increased my data set.

Sampling Strategy

I examined documents published over a thirteen year time period, from 1996 to 2008. Earlier texts on my topic were not found, suggesting that the occurrence of cybercrime at online gambling sites was a recent phenomenon, involving cases of cyberextortion (Karshmer 2005; Bednarski 2004; McMullan & Rege 2007), collusion (Arkin et al. 1999; IGDA 2004; Yan & Randell 2005), hacking (Arkin et al. 1999; McGeathy 2001; Payton 2005), money laundering (GAO 2002; Wang & Ke 2004; AGCC 2006), fraud (Arthur 1997; Kvarnstrom, Lundin & Jonsson 2000; Youn, Wan & Faber 2001), and the promotion of underage gambling (Keller 1999; Smeaton & Griffiths 2004; Andrle 2006) within this time frame.

The units of analysis for my research were documents. I employed a purposive sampling strategy which involved selecting units of analysis on the basis of project relevance. Purposive sampling was particularly relevant when researchers were concerned with investigating and understanding a phenomenon. Neuman (2003) noted

that this sampling technique was used in exploratory research and in three particular settings. First, it was used to select unique cases that were especially informative (Neuman 2003, p. 213). For instance, to explore the criminal techniques used in money laundering operations that utilize gambling sites, I selected reports published by government agencies (FinCEN, FINTRAC, FATF, GAO) because these specifically addressed the issue at hand. Second, this sampling strategy was also used to select individuals from a "difficult-to-reach, specialized population" (Neuman 2003, p. 213). This was particularly true when accessing cybercriminals, as it was impossible to list all cybercriminals and then randomly sample from the list. Instead, I used documents on hacker taxonomies, ideologies, and interviews as 'samples' to represent cybercriminals in my study. Third, purposive sampling was used when researchers wanted to identify specific cases for in-depth investigation (Neuman 2003, p. 213). The purpose was to gain a deeper understanding of a phenomenon, and not to generalize to a larger population. Although my research did not examine a particular cybercrime in depth, I used several case studies to shed light on various cybercriminals and their modus operandi. As my research explored the phenomena of online criminal organization and operation at gambling sites, the goal of my sampling strategy was to encapsulate a *relevant* range of documents that would allow me to make strategic and cross-contextual comparisons. Hence, my sampling strategy was based on themes that emerged from my literature review and preliminary internet searches.

I started with generalized search phrases, such as "internet gambling" + cybercrime, "online gambling" + cybercrime, and bookmaking + cybercrime, which revealed a variety of cybercrimes, such as cyberextortion, fraud, and money laundering.

Additionally, my literature review revealed that gambling sites were victims, perpetrators, and/or instruments of and in cybercrimes. Together, my literature review and preliminary searches informed my next set of keyword phrases. I combined different concepts creatively to generate unique search parameters, such as cyberextortion + "organized crime", "money laundering" + ecash", and fraud + "shell gambling sites". The documents retrieved through these searches guided my choice of further search parameters to obtain more specific information. For instance, when collecting documents on cyberextortion, I discovered key phrases such as 'Distributed Denial of Service (DDoS) attacks' and 'botnets', which led to the creation of a more specific search phrase: cyberextortion + DDoS + botnets. I continued to use this snowballing technique until no new keywords emerged and all relevant search phrases (48 in total) were generated [Table 1]. In doing so, I was able to generate an increased data set, conduct refined searches, and retrieve relevant data around four intersecting themes: internet gambling, cybercrimes at gambling sites, criminal techniques, and social control and governance of cyberspace with particular relevance to gambling.

Documents for gambling site *victimization* were retrieved through keyword combinations such as "cyberextortion" + "internet gambling", cheating + "internet gambling", and hacking + "internet gambling". Data on gambling sites as *perpetrators* was found using fraud + "internet gambling" and "internet gambling" + youth, while information on gambling sites as *instruments* was obtained using "money laundering" + "internet gambling". My research questions were structured around online criminal organizations and operations, which determined keyword phrases, such as "online organized crime" and "hacking techniques". The articles returned for each of the

keywords made them consistent. For example, using the "cyberextortion + organized crime" keyword combination ensured that all retrieved documents contained these keywords. Thus, this collection process helped organize the data, identify commonalities of themes, and create consistency and uniformity when conducting document analysis. Furthermore, the articles returned through searches often revealed new keyword combinations that were used for further searches. For instance, articles found using the "internet gambling + cyberextortion" keywords had words such as DDoS, botnets, etc. Thus, a new keyword combination (cyberextortion + DDOS + botnets) was created and used to retrieve more documents, which increased my data set.

I sampled documents until "thematic saturation" was achieved. Saturation occurred when the themes identified in the documents began to repeat themselves and subsequent documents did not yield new themes. In this study, thematic saturation occurred with a sample of 100 documents per keyword phrase. In general, Google searches returned 10 'hits' (links to websites or documents) per page, returning a vast number of articles per keyword search (anywhere from 4 to 1,780,000). I used the first 10 pages, i.e. 100 documents (thematic saturation criterion) for each of the 48 keyword combinations to obtain a total of 4800 sample documents. Each of these articles, however, varied in relevance and length. Many repetitions occurred in the page rankings so my actual sample size was much smaller and comprised approximately 500 documents. Overall, this procedure was a consistent means of collecting data and ensured that each category was given equal weight and consideration. In addition to internet research, I used the library resources at Saint Mary's University and Dalhousie University. Here, I accessed the library databases (EBSCO, Sociological Abstracts, etc),

several academic and technological journals (Journal of Law and Information Science, Canadian Journal of Criminology, ACM Computers in Entertainment), and relevant academic texts to supplement my internet findings with peer-reviewed scholarly material, which offered in-depth and systematic research on cybercrimes and specialized techniques. For instance, the fraud study (Kvarnstrom, Lundin & Jonsson 2000) and the collusion classification study (Yann & Randell 2005) conducted detailed studies of fraudulent and collusion activities occurring at gambling sites respectively. Thus, internet and journal database searches collectively produced a comprehensive data set.

Coding Strategy

My coding technique was based on themes that emerged from my sampling strategy, which I used to organize the raw data. I deployed a three-step coding process. First, I conducted *open coding*, where I identified initial coding categories, sub-categories, and condensed large amounts of data (Barker, Jones & Britton 1996, p. 4). All the information retrieved through this process was then filtered into the following categories: (i) internet gambling and cybercrime, (ii) organized crime, cyberextortion, and money laundering (iii) hacking and cracking, (iv) cheating and collusion, (v) fraud, non-payment of winnings, and software tampering, (vi) the promotion of underage gambling, (vii) intellectual property theft and netwars, and (viii) social control measures against cybercrime.

Second, I implemented *axial coding* where I developed connections between the categories and their sub-categories from the first coding stage by putting data back together in new ways (Barker, Jones & Britton 1996, p. 4). For example, documents collected for the 'cheating and collusion' theme had varying information (some detailed

group size, while others profiled attack types and patterns) that was not as useful in isolation. By combining this information to best serve my research objectives, however, this coding stage allowed me to develop a reasonable picture of player collusion at gambling sites.

Finally, I conducted selective coding, which involved the integration of the developed categories from the second stage to determine the relationships between them in various contexts (Barker, Jones & Britton 1996, p. 4). For example, the data on hacking techniques and cheating tactics were examined to determine commonalities in characteristics, such as type of digital attack and skill sets. Furthermore, I reviewed and examined the weak and less relevant themes from the earlier coding stages, modifying them as required. For instance, I did not find any data on intellectual property theft and netwars at gambling sites, and so this category was eventually eliminated from my research.

Data Categories

The collected data was sorted into seven areas: internet gambling and cybercrime; organized crime, cyberextortion, and money laundering; hacking; cheating and collusion; fraud, non-payment of winnings, and software tampering; underage gambling; governance, security and social control. This categorization allowed me to gather information that captured the diversity of cybercrimes at gambling sites. I identified the important features in each category that offered insights into criminal techniques and organizational dynamics. Furthermore, this process allowed me to revisit the data to identify patterns and make connections between the different categories, as well as recognize elements of my theoretical framework in the data. This, in turn, permitted me

to bring information together in new and creative ways so that it addressed my research objectives. Thus, I gained a new cut on the data, which was useful during the analytical stages of my research.

Internet Gambling and Cybercrime Data

There were numerous online articles on this topic. The keywords used were: "internet gambling" + cybercrime (23,900 articles), "online gambling" + cybercrime (53,100 articles), and bookmaking + cybercrime (2,180 articles). These searches directed me to several case studies in Canada, the UK, and offshore betting websites. Case studies were found mostly on news websites (MSNBC, CBC). These listed the online gambling companies that were attacked or had cheated customers: BetWWTS.com, CryptoLogic, BlueSquare, Paddy Power, Harrods Casino, InterBingo, InterCasinoPoker, VIP Casino, William Hill, Canbet Sport Bookmakers Internet Company, to name several. These articles provided numerous details on the nature and frequency of attacks and security measures in place (or those that were lacking) and, in turn, this led to further resource materials, such as the global scope of cybercrime, and the security solutions to the problem. These documents helped identify the nature and diversity of cybercrimes occurring at gambling sites, and guided my choice of other keywords to obtain information on these crimes. For instance, documents in this category revealed information about cyberextortion, collusion, and fraud, which I then used to generate new search phrases, such as "cyberextortion + organized crime", "cheating + online games", and "fraud + internet gambling + payouts", which generated further data for analysis.

Organized Crime, Cyberextortion, and Money Laundering Data

Many of the internet articles revealed that cyberextortion was linked to criminal organizations. Online searches were done using the keywords: "cyberextortion" + "internet gambling" (82 articles), cyberextortion + "organized crime" (32,800 articles), cybercrime + "organized crime" (122,000 articles), and "online organized crime" (1,960 articles). These articles described the organized crime characteristics of cyberextortion, such as its scope, size, division of labour, and structure. The methods used to guarantee successful operations (or not) were searched using these keywords: "online organized crime" + tactics + methods (408 articles), cyberextortion + patterns + trends (110 articles), and cyberextortion + DDoS + botnets (16,200 articles). Details on money laundering operations were obtained through keyword combinations, such as "money laundering" + "internet gambling" (68,000 articles), "money laundering" + "organized crime" (483,000 articles), and "money laundering" + "eCash" (557 articles).

Many of the online articles were from USA Today, USInfo, Eweek, Information Week (online magazines), North Carolina Wesleyan College, American University (online academia), and the Computing Research Association (computing websites). Online searches also provided formal reports such as "Virtual Criminology Report: North American Study into Organized Crime and the Internet", "Organized Crime Situation Report 2004: Focus on the threat of cybercrime", and "Organized Crime and Cyber-Crime: Implications for Business". These were highly credible resources for gathering data on the organized crime dimension of cybercrime, of which cyberextortion was but one sub-category. These documents provided accounts of how organized crime emerged in cyberspace and structured itself in this realm. In addition, searches were done at the

Saint Mary's and Dalhousie libraries, directing me to books on organized crime that contained information on the traditional forms of gambling and organized crimes, such as their characteristics, structure, and methods, which were useful in comparing terrestrial and online crimes at gambling venues.

Hacking Data

These online searches provided data about the digital methods and trends of hack attacks. The keywords used in Google to get this information were: hacking + "internet gambling" (56,700 articles), hacking + techniques (1,780,000 articles), hacking + tools (4,430,000 articles), hacking + "identity theft" (966,000 articles), hacking + software (37,500,000 articles), and hacking + motivation (1,010,000 articles). The online articles were from MSNBC, CBC, BBC (online news sources), ZDNET, Newscientist, Macnewsworld, Wired.com (online computer magazines), Internet Security Systems, Prolexic (online security companies), and the Computer Crime Research Center (online computer crime centers). They provided information on the nature of attacks, how they were organized, their frequency and timing, and who was involved.

Online searches also led to library materials, which provided useful information on the different types of attacks and the rationales for them. Works by Wall (2007), Mitnick and Simon (2006), Jewkes (2007) and Wilding (2006) served as an information repository on the nature and trends of digital methods used in general cybercrimes, such as fraud and cyberextortion. These generalized cybercrime techniques were then applied to specific crimes occurring at gambling sites in order to understand their inner workings.

Cheating and Collusion Data

These documents highlighted numerous types of cheating typologies and respective colluding tactics. The keywords used for these searches included: "player collusion" + "internet gambling" (249 articles), "cheating" + "internet gambling" (191,000 articles), "cheating" + "online games" (791,000 articles), "player collusion" + prevention (180 articles), and "player collusion" + security (1,500 articles). Several technological articles offered information on systematic collusion classifications, the use of artificial intelligence (AI) programs to defeat honest players, and the manipulation of gambling systems and software to gain an unfair advantage. White papers by gaming developers, such as the International Game Developers Association (IGDA), and gaming commission reports, such as the Alderney Gambling Control Commission (AGCC), outlined numerous cheating techniques due to system vulnerabilities and the lack of rigorous software testing and quality control. Collusion cases were obtained from websites, such as TitanPoker.com, BamBamPoker.com (online gambling sites), BBC News site (news websites), and CNET and ZDNET (online computer magazines). Secondary searches through library databases yielded journal articles on collusion typologies, abuse of security and software designs, and prevention techniques.

Fraud, Non-payment of Winnings, and Software Tampering Data

In order to find articles on the different types of fraud committed by gambling sites against their customers and licensees, I used the following keyword combinations: fraud + "internet gambling" (258,000 articles), fraud + "shell gambling sites" (4 articles), fraud + "internet gambling" + winnings (47,000 articles), and fraud + "internet gambling" + payouts (111,000 articles). These searches led me to responsible gambling

sites (BC Responsible Gambling) and news sites (Times Herald, Investor's Business Daily, and the Independent). These sites provided information on shell gambling sites, unscrupulous website operators, and the illegal sale of confidential customer information to third parties for profit. Articles obtained through the 'Gambling Magazine' website and journal articles, such as "Gambling @ Home: Internet Gambling in Canada", were used to gain information about specific cases on fraud, that identified key participants and their fraudulent techniques. Tactics used in general online fraud cases were also found on policing and consumer protection sites, such as the Royal Canadian Mounted Police, Federal Bureau of Investigation, and Internet Crime Complain Center. Library searches directed me to the Internet Gambling Report IV (Cabot 2001), and several law journals (Federal Communications Law Journal, International Gambling Studies, the Gaming Law Review, the Yale Law Journal, and the UNLV Gaming Research & Review Journal), which offered a wealth of information on several collusion activities committed at gambling sites. Academic papers, such as "Combining Fraud and Intrusion Detection – Meeting New Requirements", conducted an in-depth examination of fraud in gambling services, such as overcharging customers, denying customers their winnings, and tampering with gambling software to prevent fair play.

Underage Gambling Data

Several articles suggested that poor age verification systems for internet gambling permitted underage users to play online. The keywords used in Google to obtain this information were: "internet gambling" + underage (149,000 articles), "internet gambling" + youth (171,000 articles), "online gambling" + adolescent (75,000 articles), and "internet gambling" + youth + "identity theft" (6,850 articles). Internet searches offered

research reports published by government agencies (State of New Jersey Commission of Investigation & Attorney General of New Jersey, National Gambling Impact Study Commission, and Gamcare), outlining the ease with which youth created online gambling accounts. Library database searches yielded articles from gaming law journals (UNLV Gaming Research & Review Journal and the Yale Law Journal), that identified poor age verification systems, fraudulent use of credit cards, and technological know-how, as the prime factors determining youth gambling activities online. These issues were echoed in other journal articles, such as the Youth Gambling International Journal and the Journal of CyberPsychology & Behavior, which also described the consequences of adolescent gambling, such as problem gambling, and credit card and identity theft.

Governance, Security, and Social Control Data

This was an especially difficult topic to get precise documents on, since there were few measures currently in place by state, gambling companies, and security businesses to counter cybercrime at gambling sites. Furthermore, documents detailing successful sting operations, the observation of cybercriminal activities, and cybercrime prevention measures were not publicly available because these were sensitive and confidential in nature. Some of the keywords used in Google to search this topic were: cybercrime + combat (441,000 articles), cybercrime + police (1,270,000 articles), cybercrime + regulation (919,000 articles), and cybercrime + law (1,540,000 articles). Some of the online articles addressed the limitations of law and regulation in the context of cybercrime. For instance, the Computer Crime Research Center listed some of the difficulties in apprehending criminals online. The Canadian Department of Justice (CDJ) website had a section on 'Lawful Access Laws' which dealt with the need for up to date

laws in order to promote policing efficacy. The McConnell International Law firm had materials urging the judiciary to ensure that old laws kept up with the current times and trends. Other online articles addressed what businesses should do if they were targets of cyberextortion. These were found on news websites (MSNBC), computer crime centers (Computer Crime Research Center), and police websites (National Hi-Tech Crime Unit, FBI, and RCMP), and were especially useful in revealing resistance and protection strategies to control cyberextortion, hacking, money laundering, and fraud.

The primary source of information for private security measures was the internet. Some of the articles from initial searches revealed the names of security companies that countered cyberattacks for their clients. Here, the keywords used in the search engine were: cybercrime + security (1,580,000 articles), cybercrime + defense (1,040,000 articles), cybercrime + jurisdiction (184,000 articles), cybercrime + prevention (706,000 articles), cyberextortion + prolexic (295 articles), cyberextortion + digidefense (6 articles), DDoS + prolexic (16,500 articles), and DDoS + digidefense (242 articles). Websites of security companies such as Prolexic, DigiDefense, Symantec, McAfee, Radware, Technical Systems Testing (TST), Top Layer Networks, CISCO, and Lancope were also visited, which had specific information on products and services, as well as research reports and white papers about cybercrime and security. Prolexic and TST, for example, had articles documenting several cases of DDoS attacks on gambling sites and how they were thwarted or not. It also provided further resources for researching other case studies, successful counter-measures and the latest information on DDoS attacks and their prevention. These search results helped identify various protective and preventative measures offered by security firms.

Online searches led to formal reports by credible institutions. For instance, the "Organized Crime and Cybercrime: Criminal Investigations on the Cutting Edge" report by the Canadian Police College provided details of policing strategies to cope with the new waves of online crime. It addressed the paucity of trained personnel and the growing gap between cybercrime and policing bodies. Another report "Organized Crime and Cyber-Crime: Implications for Business" prepared by Computer Emergency Response Team (CERT), identified a series of measures that needed to be undertaken by businesses to effectively defend themselves from the growing threat of online organized crime.

These data categories allowed me to gather information systematically on the various types of cybercrimes at gambling sites and counter-cybercrime measures. Using a variety of sources that ranged from news and magazine sites, academic sites, hacker community sites, and security sites to formal reports, white papers, and journal articles, I was able to gain multiple perspectives on the multi-faceted and complex nature of these cybercrimes. Though this method gathered information-rich data that helped me gain a preliminary understanding of cybercrimes, document analysis had a few limitations that needed to be addressed.

Methodological Limitations

From the beginning of this research, I considered the pros and cons of document analysis. While it was clear that documents offered a means to explore a phenomenon, a shortcoming of this method was the "difficulty of expanding beyond what [was] documented" (Dantzker & Hunter 2006, p. 98). I encountered this problem and soon realized that acquiring *all* relevant material was not feasible. For example, self-report documents produced by gambling companies about their victimization were not

discovered in my searches. These reports probably existed, but they were not publicly available. Gambling companies feared reputation damage, loss of customers to competition, and possible future attacks, and so they were reluctant to publicly announce their victimization. Also, legal and security reports were few in number because these bodies did not wish to reveal sensitive case information to wider audiences. Thus, obtaining data on detailed sting operations, digitized investigative techniques, and technological devices used to apprehend cybercriminals, was difficult and resulted in sketchy information and only partial data for analysis. Though credible and high quality sources were used, these were select in number and this also restricted the scope and depth of my study. My thesis, however, was an exploratory study into the modus operandi of cybercrimes at gambling sites. It was not an in-depth study of cybercrimes at all, or even select, gambling sites. Where these shortcomings existed, I made a conscious attempt to obtain numerous documents in order to make inferences about this partial data. For instance, I collected reports from security industries and policing bodies that documented the use of protection services by gambling sites and generalized accounts of cybercriminal detection and apprehension. I then triangulated and coded this data using specific categories that remained faithful to my theoretical framework and research objectives, allowing me to fill in a plausible picture of cybercrimes at gambling sites.

Validity issues also posed a problem in document analysis. Was the collected data representative of the actual phenomena being studied? Neuman (2003) warned that pre-existing texts often indexed different topics, which may not necessarily capture what was being studied. Indeed, the data collected for my research did not always capture a specific cybercrime occurring at gambling sites. For example, when searching for "organized

crime and cyberextortion", I found general documents on "organized crime and cybercrime". Some of these documents represented cybercrime, not cyberextortion, but they still contained useful information to my thesis. By using purposive and snowball sampling, and methodical coding that reflected my exploratory research goals, I was able to systematically filter the documents to retain relevant information, such as the organizational dimensions of online organized crime (size, scope, division of labour, criminal techniques). While striving for absolute validity is difficult if not impossible, by harvesting pre-existing documents to obtain pertinent data, I am confident that this thesis offers an accurate if exploratory representation of cybercrimes at gambling sites.

As a majority of the documents for my study were retrieved via the web, issues of quality control, data availability, and data manipulation also arose during the course of my study (Neuman 2003). In order to ensure the use of trustworthy information, I made a conscious effort to access websites that were deemed credible, such as news websites (MSNBC), security websites (McAfee), and law enforcement websites (Canadian Policing College), all of which were professional sites and arguably had a reasonable level of reliability when compared to other types of websites. Furthermore, excellent sources for research, such as research studies, white papers, and government reports were often thought to be unavailable on the internet (Neuman 2003). While obtaining research studies on internet gambling and cybercrime was difficult because little work had been done in the area, I was pleasantly surprised to find prime resources that were not available in conventional forms. Online peer-reviewed journals, formal reports produced by government, security, and policing bodies, and white papers by gaming developers and gambling commissions, offered excellent materials for my study. To be sure online

resources may have been modified, moved, or terminated, but I ensured that this instability did not impact my research. I catalogued each document's online address or uniform resource locator (URL), retrieval date, and source (magazine, news, government, private sector), and I printed a hard-copy of each online article, which retained information that may have otherwise changed or expired. This ensured that my data set remained stable during the coding and analytical process. By consciously accessing credible sites and using systematic collecting strategies, I am confident that I obtained rich and recent data for exploring the dynamic phenomenon of cybercrimes at gambling sites.

There could, of course, be keyword combinations that I did not consider and that might have resulted in a more detailed search with potentially different findings. My research, however, was exploratory in nature and I created an exhaustive set of search phrases that allowed me to tap into the understudied area of cybercrimes at gambling sites. Initial keywords retrieved documents that revealed new concepts which were then incorporated into subsequent search terms. This snowballing technique was extensive; all possible keyword combinations I could imagine were used to retrieve documents for my study. I am sure that these keywords helped identify the types of cybercrimes, their organizational dynamics, criminal techniques, and rationales.

Combining document analysis with other research methods, such as surveys and interviews may have also revealed different and detailed insights. Both interviews and surveys, however, would require carefully designed questions, proper operationalization (accurate measurements of desired factors) techniques, and the ability to identify and access the right participants. Though these methods could have been employed, using

them in conjunction with document analysis would require long term planning, ethics clearance, and an extended time frame, which were beyond the time frame of my research project. Furthermore, structuring the various components (questions, operationalization) of these methods necessitated appropriate background information on the topic. Document analysis enabled me to generate precisely this preliminary information, which can better inform other keyword phrases and/or other research methods for future in-depth studies.

I also recognize that using alternative search engines (Yahoo or AltaVista) could have resulted in different articles that provided new information and therefore, a different analysis. My research, however, was not exhaustive; it opened up the area of online criminal organization and operation. I conducted my exploratory study by sampling documents that represented cybercrimes at gambling cites. Unlike other search engines, Google retrieved documents that were ranked according to their *relevance*, which fitted nicely with my purposive sampling strategy. As Google offered state-of-the-art search algorithms, crawlbots, and PageRank technology, I am confident that the web was mined with precision to retrieve the best possible data. My research findings can serve as a foundation for future studies, whereby different search engines, keyword phrases, and research methods can be used together to produce more focused studies.

Conclusion

I argued that document analysis provided an appropriate means for gaining a plausible first picture of cybercrimes at gambling sites. Document analysis was chosen because its ability for 'discovering' phenomena fitted nicely with the exploratory nature of my research. Each step in this methodology reflected my research objectives, which

ensured that my data remained true to my research interests. I employed a creative and systematic sampling and coding strategy that ensured the collection and categorization of rich and credible data from an assortment of sources. I combined and triangulated this data in innovative ways to filter the collected data to meet my research interests. As we shall see in the next two chapters, this allowed me to piece together the assortment of criminal techniques used by, and the different organizational dynamics of, cybercriminals.

Chapter 4

Doing Cybercrimes

Introduction

A majority of online casinos, lotteries, and bookmaking sites serve as alleged "playgrounds" for cybercriminals (CERT-LEXSI 2006, p. 7). This chapter presents my findings about the various criminal techniques used by an assortment of cybercriminal types, such as hackers, cheaters, cyberextortionists, and gambling sites themselves. First I examine how hackers and cheaters exploit system vulnerabilities, manipulate software, and intercept data flow and wire transfers at gambling operators. The second section discusses how gambling operators and cheaters use rootkits and toolkits respectively to commit cybercrimes. The third section details how cheaters, cyberextortionists, and money launderers use artificial intelligence programs, networks of compromised computer systems, and infected machines respectively to target gambling sites. The fourth section examines how fraudulent gambling operators, money launderers, and hackers use shell sites, complicit sites, and cloned sites to further their online criminal pursuits. I conclude by identifying the characteristics of these techniques and raise questions as to their relation to criminal organization.

Exploitation, Manipulation, and Interception

Cybercriminals typically exploited bugs in gambling systems, tampered with gambling software, and intercepted information flowing between gambling servers and customers. Hackers searched for vulnerable gambling sites or software, which were readily accessible and easy to compromise. Then they used specialized criminal techniques that attacked the operating systems, networks, databases, and other system

applications of these sites and software, which were used to affect the behaviour of online games (IGDA 2004, p. 73).

Hackers often exploited bugs or loopholes in gambling programs, without the modification of game code or data (Yan & Randell 2005, p. 4). Here, cybercriminals used their technical expertise to find and abuse gaming software bugs. Personalized tactics to detect these loopholes involved playing games with an eye for malfunctions. These bugs were studied, noted, and linked in order to achieve optimal exploitation. Software problems were a well-known "security risk often overlooked by companies obsessed with firewall and cryptography" (Arkin et al. 1999, p. 2; McGraw & Hoglund 2007, p. 31). Often, game designers did not subject their software to adequate quality testing procedures and sometimes detecting all possible bugs or loopholes was impossible (IGDA 2004, p. 74; Arkin et al. 1999, p. 2). For example, a serious flaw existed in the implementation of the random number generator (RNG) in the Texas Hold 'em software distributed by ASF Software, Inc. (McGraw & Hoglund 2007, p. 28). RNGs were used in several online games to ensure unpredictability and fairness. In such programs, the entire security relied on picking a random number or *seed* in a non-predictable manner (Arkin et al. 1999, p. 9). The flaw in the Texas Hold 'em software existed in the shuffling algorithm used to generate each deck; the code seeded the RNG with the "number of milliseconds since midnight according to the system clock", making the outcome of the RNG easily predictable (McGraw & Hoglund 2007, p. 29). Cheaters easily calculated the exact deck being used for each hand, which gave them extra knowledge, placing them at an unfair advantage over other players. The cheater therefore knew the cards in every opponent's hand as well as "cards that made up the flop (cards placed face up on the table

after rounds of betting). A cheater knew "when to hold 'em and when to fold 'em" every time" (McGraw & Hoglund 2007, p. 29). This lack of randomness led to "biased card distribution and predictable consecutive deals", which made the outcome of the game known to attentive cheaters who then bilked honest players of money or playing credits (Yan 2003, p. 3).

Cybercriminals utilized their technical and programming skills to modify or tamper with the actual game code, data, or RNG. Some hackers developed software that (i) determined "the forward progress of the ... RNG in a gambling machine", and (ii) decoded the "RNG seed values and mapping algorithm of the machine" to disrupt the game (McMullan & Perrier 2003, p. 15; Arkin et al. 1999, p. 8). Consider the case of CryptoLogic Inc., a Canadian software company that developed online games for casinos. In August 2001, hackers cracked into one of the company's gaming servers and altered one of its programs, disrupting the play of "craps and slots" so that customers always won (Warner 2001, p. 1). The gaming software was manipulated to ensure that "every roll of the dice in craps turned up doubles, and every spin on the slots generated a perfect match; ... in the case (of slots), it was coming out cherries across the board" (Warner 2001, p. 1). In the few hours of disruption, approximately 140 customers won $1.9 million and were allowed to keep the money, which caused significant monetary losses to the gambling company (CryptoLogic 2001, p. 17; Warner 2001, p. 1).

Data flow between gambling sites and their customers was often interrupted by cybercriminals to intercept their financial transmissions, steal financial information, and conduct unauthorized transactions. Hackers diverted wire transfers and funds and 'stole

bets' without detection. As Cabot (2001) suggested, a customer wagered $100 electronically; the hacker could intercept this wager and then credit:

> $90 of the wager to his own account. Instead of the $100, only the remaining $10 bet is sent to the Internet site operator. To avoid detection, the thief would then intercept the returning transmission from the site operator, and alter it to show the bet was $100. If the player won, the thief would credit his "phantom" account by $100. If he lost, neither the home user nor the site operator would realize that $90 was diverted... The home gambler will assume he lost the $100 bet, while the site operator will assume the gambler lost a $10 bet (p. 31).

Fund transfers were not the only events to be intercepted. When players were engaged in online gambling, information packets were exchanged between them. If these packets were transferred in plain text, players cheated by "eavesdropping on packets and inserting, deleting, or modifying game events or commands transmitted over the network" (Yan & Randell 2005, p. 3; Yan 2003; p. 3). Consider the 1995 OKbridge.com Knockout Tournament cheating case. One team comprised two American and two European players, who exhibited non-expert level play. Yet, this team reached the final stages of the tournament and defeated reknowned experts in the semi-finals (Eskes 1996, p. 3). The losing expert team had a "very unpleasant feeling about the match ... They [cheaters] didn't play great, but at the critical moments they made some remarkable good decisions. Their play was sometimes so unlikely, that it literally made me sick" (Esekes 1996, p. 3). When an international Conducts & Ethics Committee investigated this case, it found approximately 20 instances of odd 'bid-and-play' (Esekes 1996, p. 3). The committee concluded that one member of the cheating team was playing with 'unauthorized information'. A second cheating case at OKBridge occurred during another Knockout tournament, when one team noticed "several unusual and successful actions by ki [opponent] during their match" (Goldsmith n.d., p. 1). When the Conducts & Ethics

Committee's investigated, they found that ki's actions were "beyond belief" and "incomprehensible without illicit information" (Goldsmith n.d., p. 4). In both these cases, cheaters intercepted the network traffic to eavesdrop on the cards held by their opponents.

Another example of data interception was illustrated by the 2007 AbsolutePoker.com scandal. The site was located in the Kahnawá:ke Mohawk Indian territory outside of Montreal. Marco Johnson, a poker customer at AbsolutePoker.com requested a history of the cards he was dealt during a high-stakes game because he suspected unfair play (Goldman 2007, p. 1; Levitt 2007, p.1). Instead, he received a file that documented every player's hand histories, email addresses, and IP addresses (Levitt 2007, p. 1). This document revealed that at each table the user 'Potripper' played, another user '#363' was present but invisible to other players at the online poker table. Potripper only folded twice before this 'observer' entered the game, but then did not "fold a single hand before the flop for the next 20 minutes, and then folded his hand pre-flop when another player had a pair of kings as hole cards!" (Levitt 2007, p. 1). This implied that #363 watched every subsequent hand played by honest customers and conveyed this 'unauthorized information' to Potripper (Goldman 2007, p. 2). This collusion permitted Potripper and #363 to steal between $500,000 and $1 million from other players over a six week time period (Goldman 2007, p. 3; KGC 2008, p. 1).

Rootkits and Toolkits

Rootkits were commonly used by cybercriminals to conduct their digital attacks. Rootkits were collections of tools that gave hackers administrator-level access, or 'root' access, to computer systems (McAfee 2006, p. 3). Rootkits incorporated malware (malicious code), such as Trojans, worms, and viruses, which concealed its presence and

activity from users and other system processes (McAfee 2006, p. 3). Trojans were programs that appeared benign on the surface, but harboured malicious code within (McAfee 2006, p.4). Worms were malware that replicated by spreading copies of themselves through shared networks autonomously without any human intervention (McAfee 2006, p. 4; Symantec 2000, p. 1). Unlike worms, viruses were spread through human actions, such as running an infected program or opening a malicious email attachment, and stole sensitive information, blocked system resources, or tampered systems data (McAfee 2006, p. 4; Symantec 2000, p. 1).

Trojans were preferred by malware authors, as they were not detected by network defenses and firewalls, and were well-suited to meet the objectives of hackers by performing multiple functions (Symantec 2007b, p. 19). As Trojans did not propagate themselves, they allowed hackers to execute targeted attacks and escape notice, which increased their effectiveness: "the longer the threat [remained] undiscovered in the wild, the more opportunity it [had] to compromise computers before measures [were] taken against it" (Symantec 2007b, p. 19). In 2005, for example, the online gaming tools vendor CheckRaised distributed legitimate software packages with a hidden malicious rootkit (Naraine 2006, p. 1). This rootkit contained a spying Trojan, 'Backdoor.Win32.Small.la', which was built into CheckRaised's Rakeback calculator application (RBCalc.exe) that helped online poker players keep track of scaled commission fees taken by site operators (Naraine 2006, p. 1; Sturgeon 2005, p. 1). This rake calculator was offered as an executable file that players downloaded and ran on their systems to calculate the rake from hands they previously played (Naraine 2006, p. 1). When the program was run, however, it silently installed other files into the machine's

system directory to monitor running processes and spy on connections to several online poker sites (Naraine 2006, p. 1; Sturgeon 2005, p. 1). The Trojan's main file installed the "driver ndsdavsrv.sys" program, which concealed its "processes and the registry launchpoint" from unsuspecting users (Turkulainen 2006, p. 2). Another hidden file initiated keylogger scripts that gave hackers access to the user's login details (Sturgeon 2005, p. 1). Furthermore, these files connected to servers that were remotely operated by hackers, who then sent further instructions, such as the downloading of malicious files, the uploading of stolen information, the termination of the Trojan, and the retrieval of application screenshots (Naraine 2006, p. 1). Given this information, the hacker logged in with the compromised user's account and then played poker badly against his real account, thus making money at the victim's expense (Naraine 2006, p. 2; Sturgeon 2005, p. 1). The CheckRaised's Trojan also allowed hackers to spy on connections to other poker applications, such as "mppoker.exe, poker.exe, gameclient.exe, ultimatebet.exe, absolutepoker.exe, mainclient.exe, pokerstars.exe, pokerstarsupdate.exe, partypoker.exe, fulltiltpoker.exe, pokernow.exe, multipoker.exe, empirepoker.exe and eurobetpoker.exe", which revealed customers' usernames, passwords, and account information (Naraine 2006, p. 2).

Gambling sites also installed malware via their own programs to prevent their customers from gambling at competing sites. The casino download of Gambling Federation was a case in point. Once the company's software was downloaded, an embedded Trojan within it blocked customers' access to other operators' sites (GRP 1999, p. 1). The Trojan blocked www.theblackjacktable.com, www.casinoxo.com, and www.royaldutchcasino.com; these sites could not be accessed and a 'website not found'

error was displayed in customers' web browsers (Casinomeister 2005, p. 2). Hackers often developed Trojans that had numerous built-in evasion techniques, such as (i) polymorphism: the malware changed its "byte pattern when it [replicated], thereby avoiding detection by antivirus programs, (ii) metamorphism: the malicious code changed itself autonomously, and (iii) packers: the file size of the malware was reduced, which made its detection by antivirus programs difficult"; these tactics made Trojans flexible, durable, wider in scope, and undetectable (Symantec 2007b, p. 25).

Not all cybercriminals had the technical expertise needed to create rootkits; some individuals also used 'how-to-do-it' manuals that were sold online. For instance, Silverthorne Publications, Inc. (SPI) facilitated cybercrime by offering the 'Online Gambling Toolkit' manual, which was available for purchase as a hard-copy or an e-book for "$59.97" (SPI 2006a, p. 1). SPI advertised:

> Once you have it [manual], you will know exactly where to play, which games are best, and you will have the exact strategy to maximize your winnings. In addition, you will receive a step-by-step plan, with complete examples so that you will know exactly how to start winning $5,000 a week or more. You will even learn how to expand your winnings to even higher levels. Using this special technique you can easily win $10,000 or more a week. If you have ever wanted to win a fortune in a short time period, this is your chance! (SPI 2006b, p. 16).

Finally, this manual came with an 'ironclad guarantee', which gave customers a one-year trial period to evaluate the strategies outlined in the manual, and even offered a complete refund to unsatisfied customers (SPI 2006b, p. 22). Other individuals purchased pre-packaged toolkits that automated most of the technical work (Westervelt 2007, p. 1). These toolkits were sold by cybercriminals who advertised their services on popular hacker forums (Jellenc & Zenz 2007, p. 42). As one toolkit site stated: "You don't have to have a fancy array of hacking tools to break into a site – but they can make life a lot

easier. Do you really want to try and capture network packets and decode the hex values by hand? Thought not" (DarkAge n.d., p.1). Toolkits were collections of programs that were a hacker's "bag of screwdrivers, spanners, and – where needed – a bloody big hammer" (DarkAge n.d., p.1). Consider the 'HoldemGenius' toolkit for online poker, which saved players time and energy by calculating all possible poker odds, and used advanced mathematical algorithms to compute multiple variables, such as the opponents' position and fold depth (HoldemGenius 2008a, p. 1). The 'Pot-Odds Chart' was used by advanced players to instantly see their pot odds, odds of drawing out, and odds of winning [Figure 2] (HoldemGenius 2008b, p. 2). HoldemGenius.com was a fully functional site, offering FAQ and Tutorial sections for current customers. The site also catered to potential customers by advertising how their software supported over 100 online poker rooms (PokerStars, Full Tilt Poker, BoDog, Party Poker, Titan Poker, AbsolutePoker), and even demonstrated their product's superiority over another online poker odds calculator, 'Texas Calcultem'. Furthermore, toolkits also automatically received updates on newly found system vulnerabilities (Westervelt 2007, p. 1). The HoldemGenius software was continuously updated; the latest update (v. 1.3.09) was released on March 27, 2008 and improved the previous version by offering bug fixes in Party Poker, FullTiltPoker, and AbsolutePoker, 'auto-resizing' in TitanPoker and CarbonPoker, and supporting 2 and 9 player games at BoDog.com (HoldemGenius 2008c, p. 2-3). Finally, HoldemGenius also offered support to their customers through online support forms, which were answered within two business days (HoldemGenius 2008d, p. 1-2). While these software programs *aided* the players in their game, other programs *played* the game for cheaters, as discussed next.

Smart-Bots, Zombie-Bots, and Botnet-Armies

Cheaters often used special digitized skills and personalized criminal methods that employed automated techniques and artificial intelligence (AI) technology. AI software such as 'aim-bots' or smart-bots were tools that cheaters used to optimize their actions and were considered as forms of cheating, even if they did not otherwise break any rules (IGDA 2004, p. 73; AGCC 2006, p. 29). Poker-bots were smart-bots that connected to gambling servers pretending to be real players. These programs were designed specifically to play the optimal strategy for online gambling and therefore gave the cheater the upper hand over other players (AGCC 2006, p. 29). One such poker-bot, 'PokerSmoke' advertised:

> It's a hands-free, robotic poker player that's been deviously programmed to play a level of professional poker that you, yourself, could only dream of. It makes all of the right moves, always at the right time, to suck up consistent profits from the weakest and strongest players alike. In short, it's unstoppable! (SmokePoker.com 2008, p. 2).

The successful design of such bot software depended on two factors: (i) the characteristics of the game, and whether the game could be designed as a computable problem, and (ii) the sophistication of AI research into such forms of gambling (Yan & Randell 2005, p. 3; Brunker 2004, p. 2). Indeed, PokerSmoke incorporated a sophisticated decision engine that combined advanced neural network technology with the most accurate "opponent modeling system", which evaluated all possible outcomes and instantly predicted the cheater's chance of winning (SmokePoker.com 2008, p. 3). Furthermore, poker-bots also allowed players to participate in several games at the same time (AGCC 2006, p. 29; SmokePoker.com 2008, p. 3). In online poker, bots only 'played' under the supervision of a human: "the cards may be chosen by the bot

according to probabilities computed by the bot, but the bot cannot play without a human 'baby-sitter'" (Goelle & Ducheneaut 2005, p. 3). The user of PokerSmoke had to "simply click start" and the poker-bot monitored the user's "poker tables and automatically, memorize your opponents' game style, recognise their betting patterns, calculate your pot odds and hand odds, identify profitable decisions and finally play your cards, in the best possible way, on auto-pilot!" (SmokePoker.com 2008, p. 3). The cheater was also allowed to customize the playing level; PokerSmoke was completely configurable to the user's playing preferences: "play tight, loose, aggressive, or passive!" (SmokePoker.com 2008, p. 3). Furthermore, bot-architects often tested their programs against existing gambling systems to determine their performance level. For example, the developers of PokerSmoke provided free downloads to test their bot's performance. As more players tested the bot, the better its decision engine became which, in turn, developed the bot's precision in the game (SmokePoker.com 2008, p. 5).

Cybercriminals also used malicious bots for more complex attacks. Bots were programs that were covertly installed on a victim's machine that completely allowed the criminal to access the machine remotely (Symantec 2007b, p. 14; McAfee 2005, p. 12). Bots were typically introduced via computer viruses, such as SoBig and MyDoom, which installed 'back door' programs on the victim's machine. The hacker then used these programs to install a 'bot' on the compromised machines or 'zombies'. These zombie-bots were then awakened from dormancy at the hacker's will. An active zombie was one that carried out at least one attack per day (Symantec 2007b, p. 14). This attack was not necessarily continuous; a single zombie was active on different days (Symantec 2007b, p. 14). The zombie's lifespan was determined by the amount of time that lapsed between its

first use and until the time the zombie no longer attacked for 30 days, indicating that the compromised machine was fixed (Symantec 2007b, p. 15). Bot owners often responded to law enforcement threats by altering and tweaking their zombies; bots often assumed new functionality by upgrading to the latest codes and features (Symantec 2007b, p. 14).

Acquiring zombie-bots was the first stage of a three-step Distributed Denial of Service (DDoS) attack that was used in the cyberextortion of gambling sites. The second stage involved creating a bot-network or a botnet-army, which was a collection of these infected machines that had been "compromised weeks or months earlier by attackers" and that could be "centrally controlled and used to launch simultaneous attacks" on websites worldwide (McAfee 2005, p. 12). Known as 'herding', a cybercriminal issued orders to its zombies, directing them to send messages simultaneously to the targeted gambling website (Ratliff 2005, p. 3; Paulson & Weber 2006, p. 52). The targeted site was then inundated with requests, which consumed all available resources (disk space and CPU time) and disrupted "traffic monitoring, bandwidth capability, or physical network components" (Paulson & Weber 2006, p. 53). The site was thus overwhelmed with requests and was slowed down to a crawl, resulting in the Distributed Denial of Service (DDoS) attack [Figure 3].

Botnet-armies were used in numerous ways to execute a variety of DDoS attacks. SYN attacks bombarded the gambling site with data traffic to such an extent that it had to cease its operations. The targeted site sent back an acknowledgement to each source of the data traffic, but never got a response. This resulted in several "bogus connection requests" which were indistinguishable from legitimate customer requests, thereby allowing fake traffic to swamp the website (Golubev 2005, p. 3). Smurf attacks used

gambling sites against themselves. Here, cyberextortionists sent an "IP ping packet (or 'echo my message back to me')" request to the targeted site. The return address in the packet, however, was that of the targeted site itself, and not the cyberextortionists' real address. Thus, when several ping packets were directed at the victim website, the site bombarded itself with a DDoS attack (Golubev 2005, p. 4). UDP flood attacks or "fraggles" were more sophisticated strategies involving forged "UDP echo and character generators" that were then used to connect the echo service of one computer to the character generator of another machine (Murphy, Pender, Reilly & Connel 2005, p. 1). Once connected, these two machines relayed messages back and forth consuming the entire communication bandwidth and eventually slowing the gambling site to a crawl. Legitimate players received the internet equivalent of a busy signal indicating that the company's servers were not responding. Finally, Trinoo attacks created a domino effect on targeted gambling sites. A master program controlled by cybercriminals commenced the first set of attacks. The program then simultaneously sent corresponding orders to a waiting bot-net army who, in turn, launched an accompanying zombie-based UDP attack on the targeted site, thereby denying its customers any gambling services (Murphy, Pender, Reilly & Connel 2005, p. 2).

The final step in the cyberextortion process involved the delivery of an email to the targeted site demanding money in return for protection from further attacks: "Dear wwts, As you can see your site is under attack. We have found a problem with your network" (as cited in Karshmer 2005, p. 1). The attackers then insisted that the gambling site wire $40,000 to them: "You will lose more than $40k in the next couple of hours if you do not resolve this problem" (as cited in Karshmer 2005, p. 1). If the targeted site did

not pay up, the perpetrators continued their attacks, and the site suffered further monetary losses. Numerous gambling sites were subjected to DDoS attacks. The cases of Canbet Sports Bookmakers, BetCris, Multibet, and Grafix Softech were illustrative. Canbet Sports Bookmakers suffered a DDoS attack during the Breeders Cup, which cost it more than £100,000 in revenue for each day the site was shut down (Jellenc & Zenz 2007, p. 34). In 2003, one extortion network demanded $40,000 in 'protection money' from BetCris via email: "if you choose not to pay for our help, then you will probably not be in business much longer, as you will be under attack each weekend for the next 20 weeks, or until you close your doors" (Ratliff 2005, p. 4). BetCris did not pay up, and it took the cyberextortionists less than 20 minutes to take down the site (Ratliff 2005, p. 4). In 2004, the CEO of Multibet also refused to give into the ransom demands of cyberextortionists; the site was attacked four times and his business was interrupted for 20 days until he wired the protection money to an East European bank account (Anon 2004). Thus, targeted sites often agreed to the extortion payments, fearing additional damage. In 2003, Grafix Softech, which hosted 120 gambling sites worldwide, was shut down via DDoS attacks by a Russian-based cyberextortion network. The company, like BetCris and Multibet, paid off the ransom demands, which was seen as insignificant when compared to the loss of revenues and operational records (Walker 2004, p3). Some attacks were timed to occur with large sporting events, such as the Super Bowl, March Madness, and the Grand National, when the betting activity was highest, and when a DDoS attack could rob gambling sites of "millions of dollars worth of bets" (Warner 2001, p. 2). Indeed, the cyberextortion of gambling sites was best summed up by a security specialist who noted:

"I've seen well-engineered hack attacks coordinated with very well engineered extortion attacks", which clearly indicated the sophistication of these threats (Warner 2001, p. 2).

Cyberextortion attacks exhibited regenerative qualities. Compromised machines controlled by hackers were easily redeployed. If a bot-net army no longer served its purpose, another several hundred machines were infected to take their place within a few hours of the attack: "like the mythical Hydra, once one head has been lopped off, another quickly grows back" (Morgan 2005, p. 3). For instance, in January 2004, attacking bot-nets compromised about 2000 innocent computers; by May of 2004 the number had risen to more than 60,000 machines (Biever 2004, p. 1). With the use of dispensable bot-nets, DDoS attacks became "a piece of cake to orchestrate from a vast ad hoc network" that compromised gambling sites (Biever 2004, p. 1; Warner 2001, p. 2). Furthermore, bot-nets had a 'self-destruct' mode; as one security expert observed, the "attacker might have set up a booby trap so that the botnet goes ballistic if someone else tries to control it" (Skoudis 2007, p. 1).

Bots were also used to launder money at gambling sites. Cybercriminals stole batches of credit card numbers and for each number opened an account with a gambling site. Next, they entered online poker rooms with an unsophisticated 'bot-player'. A criminal associate then entered the room to compete against, and defeat, this bot-player, thereby allowing the money to 'change hands', with both participating members getting shares of the profit (Onlinepoker-news.com 2007, p. 1). Security experts noted that botnet armies were also used in money laundering schemes (as cited in Sullivan 2007, p. 1). These 'battalion of bots' posed as players and flooded online casino game rooms at the behest of the money laundering group. Each bot was given small amounts of dirty money,

and was programmed to wager, pick cards, and fold if necessary. The bot-herder then took the last seat in the fixed game, won against the bot-players, cashed out, and transferred these 'winnings' from the site's payment processor (Sullivan 2007, p. 1).

Phantom Sites, Complicit Sites, and Spoofed Sites

Many gambling sites were located offshore, and had declared suspicious bankruptcies, or appeared and disappeared with regularity (Zacharias 2004, p. 4; CERT-LEXSI 2006, p. 1). Customers who dealt with these sites were rarely paid their winnings or even given back their initial deposits (Cabot 2001, p. 33; Penenberg 1998, p. 1). Site operators transferred funds deposited by customers into their own accounts and then shutdown the site; about 70% of gambling sites were fake. The operators of these 'phantom' sites had no intention of returning deposits or paying out rightful winnings to their customers (Cabot 2001, p. 33; Zacharias 2004, p. 4; Cody 2001, p. 3). Customers registered with their credit cards or wired funds into these phantom sites, and the site operators then plundered customer accounts (Heinrichs 2001, p. 1). A case in point was that of Jeffery Pealer, who was cheated by GlobalSportsNet (Kelley 1997, p. 1; Arthur 1997, p. 1). He was told that his winning cheque was mailed to him, but never received it. When trying to contact the company, no officials or employees were available and he learned that that the company was not licensed to operate (Kelley 1997, p. 1). These cybercriminals had the technical and programming skills to design "mind-blowing websites with the fanciest graphics, but absolutely no head office" (Arthur 1997, p. 1; Shaw 2004, p.2). Indeed, the Antigua and Barbuda Free Trade and Processing Zone Commission had no knowledge of the company's existence or "any person or entity representing" it (TheGames 2007, p. 1). The license displayed on GlobalSportsNet's site

was fraudulent; it was never issued by the Free Zone Commission. Other online betting operations were also notorious for shorting their customers. In 1997, a Panamanian-based sports booking website, 'Fallons' disappeared, leaving its customers without their winnings. 'Bingo World' also collapsed and hundreds of its customers were left with defunct company phone numbers and e-mail addresses. As one industry insider noted, these "unpaid winnings [totaled] more than $500,000" (as cited in FACC n.d., p. 3).

Money laundering was conducted through either legitimate or complicit gambling sites. Organized crime groups frequented legitimate gambling sites as these facilitated their money laundering operations. The electronic payment mechanisms offered by gambling sites were often used to transfer funds generated through criminal activities. Two forms of electronic payment facilities were generally used, cyberpayment systems providing digital cash or e-cash, and internet banking (Wilson & Molander 1998, p. 27). Both offered increased speed of transactions, the ability to transfer funds across geographical barriers, and low detection to regulatory and law enforcement bodies, giving criminals the potential means to "bypass traditional money laundering controls, possibly creating an ideal vehicle for money laundering" (GAO 2002, p. 38; Wilson & Molander 1998, p. 27). Money laundering usually involved multiple transactions to mask the origin of financial assets used by criminal enterprises. The goal was to convert large sums of money obtained through illegal means into more manageable and legal monetary instruments or other assets, without leaving an identifiable paper or electronic trail (FinCEN 1998, p. 1). The money laundering process typically occurred in three stages: (i) placement – illegal funds were placed into financial institutions through deposits, wire transfers, or other means, (ii) layering – several complex financial transactions moved

money to such an extent that it eradicated the money trail so that it could no longer be associated to criminal activity, and (iii) integration – legitimate transactions were used to disguise illegitimate funds. Money was placed back into the economy under the guise of normal business earnings, thus blurring the lines between legitimate and illegitimate funds (McDowell & Novis 2001, p. 1; FinCEN 1998, p. 2). Gambling sites were used as instruments in the 'layering' stage of the money laundering process. Here, the gambling site, like the Chop, Hundi, or Hawallah bank in traditional money moving schemes, became an important component of transferring funds.

Offshore betting sites in Curacao, the Netherlands, Antilles, Antigua, and the Dominican Republic were linked to money laundering operations by the FBI (Lilley 2003, p. 123). Cybercriminals layered illicit funds in several ways. One strategy was to deposit funds into fake accounts with a legitimate gambling site. 'Players' then placed small wagers to portray themselves as legitimate customers to the site operator. After a few plays, players withdrew the remaining illicit funds from the fake account. The layering stage of the money laundering process was successfully done as the transaction trail was seen as a legitimate online gambling transaction, where illicit and legitimate funds were mingled (GAO 2002, p. 36). The only money the player 'lost' was the processing charge and other site fees, while the remaining money appeared as legitimate winnings (GAO 2002, p.36). Another strategy involved a tactic called 'chip dumping' (AGCC 2006, p. 28). Fraudulent monies were deposited into a fake customer account. These monies were 'lost' to a colluding associate, who then cashed out these dumped 'winnings' to his or her credit card, further complicating the money trail and offering another successful layering technique in the money laundering process. Yet another

technique to mask illicit funds was to not always cash out winnings immediately (GAO 2002, p. 28). Fake customer accounts were created for the sole purpose of being used as a temporary storehouse for illicit funds (GAO 2002, p. 28). These funds were eventually transferred to offshore accounts or cashed out and 'reinvested' elsewhere to add another level of complexity to the layering process (GAO 2002, p. 28). Some cybercriminals used legitimate offshore gambling sites to launder funds. Consider the 2005 money laundering indictment against WorldWide Telesports, Inc. (WWTS) and Soulbury Ltd. From 1998 to 2005, William Scott and Jessica Davis operated WWTS through which they illegally enticed American gamblers to place wagers on online casino games and sporting events. Wagers were placed on baseball, basketball, football, hockey, and other sports via toll-free phone numbers, www.BetWWTS.com, and "other Internet websites" operated by Scott and Davis (DOJ 2006, p. 1). According to the indictment, Scott hid his personal profits from this illegal gambling enterprise at Soulbury Ltd., a shell corporation, and several foreign banks (Ames 2006, p. 1).

Money laundering was also conducted through complicit gambling sites. Cybercriminals often developed their own gambling sites for the sole purpose of laundering money (GAO 2002, p. 37). Consider the 2006 case of the online gambling operation headed by James Giordano, which was exposed after police cloned his hard drive and monitored his phone activity. Giordano was unaware that his computer had been tampered with and that his actions were being tracked by law enforcement. Police discovered that members of this illicit operation were technologically adept and proficient in laundering unlawfully earned proceeds through online casinos, shell corporations, and bank accounts in Central America, the Caribbean, Switzerland, and

Hong Kong (NorthCountryGazette 2006, p. 1). One of the members developed a sports betting site 'playwithal.com', specifically designed to meet the needs of the Giordano family (NorthCountryGazette 2006, p. 3). This site allowed approximately 40,000 customers to place bets on football, baseball, golf, and other sports (Venezia, Martinez & Livingston 2006, p. 1). The bettors used the playwithal.com site as a wager sheet to place their bets, and then paid their losses or collected their winnings in face-to-face meetings with the bookies (Venezia, Martinez & Livingston 2006, p. 3). In another case, organized crime groups hired computer programmers who were assigned the task of creating phony gambling sites with flawed software. The site 'operator' programmed the gambling software to "react to a specific password or sign-on command, automatically taking a percentage of the deposit and cloaking it as a gaming loss" (GAO 2002, p. 37). This was seen as the operator's service fee or commission for laundering the illicit funds. Furthermore, these complicit sites required legitimate gamblers in order to prevent the site from being discovered as an illegitimate site by law enforcement officials (GAO 2002, p. 37). These complicit sites often changed their hosting providers and country of business registration several times a month; some even disappeared for short time periods and later reappeared under entirely different credentials (CERT-LEXSI 2006, p. 4).

Cybercriminals also mimicked legitimate gambling sites and used phishing attacks to lure customers. When players joined loyalty schemes, they supplied detailed personal information, such as their names, addresses, telephone numbers, dates of birth, and genders (Griffiths 2003, p. 563). Players were then given userIDs and passwords, which were unique identifiers for each gambling customer. Customer accounts not only contained all their confidential information, but also contained playing credits or money.

'Phishing' involved online identity theft, by obtaining this confidential customer information that was stored in the gambling company's database (Emigh 2005, p. 6). Phishing attacks were done in several ways: (i) the deceptive attack, where users were tricked by fraudulent messages into releasing their information, (ii) the malware attack, where malware (malicious software) compromised and/or retrieved confidential user information, and (iii) the DNS-based attack, where the IP (computer) addresses of sites were altered to send victims to a fraudulent server (Emigh 2005, p. 6). Hackers installed "sniffers", Trojan horse programs, or cheat codes, through email and malicious websites, which were then used to hijack game sessions, steal users' passwords and credit card numbers, and compromise users' computer systems (McGeathy 2001, p. 127; Chen et al. 2005, p. 3).

All phishing attacks fitted into a general schema, as illustrated by the case of PartyPoker.com, the world's largest poker website (Emigh 2005, p.2; Thompson 2007, p. 1). First the phisher prepared for the attack by designing the phishing scam. The phishers created a clone of the PartyPoker site and hosted it on their own servers. Second, the phisher chose the appropriate medium to lure victims; PartyPoker's customers were sent emails warning of US legislation that would affect online poker players:

> Dear poker player, Information for US and all over the World based customers on the passing of the Unlawful Internet Gambling Enforcement Act of 2006. On September 30, 2006, the United States Congress passed The Safe Port Act. That measure also contained certain provisions known as the Unlawful Internet Gambling Enforcement Act of 2006. On October 2, 2006, Party Gaming made an announcement regarding the impact the act would have on business when, as expected, it is signed into law (as cited in Thompson 2007).

This email included a link to the well-designed clone of PartyPoker's login page. Third, victims performed an action through which they became vulnerable to an

"information compromise" (Emigh 2005, p. 2). PartyPoker users clicked on the link in the email, and were directed to the fake site. Fourth, victims were prompted for confidential information; PartyPoker customers disclosed their personal account details by logging into the cloned site. Fifth, this sensitive information was relayed back to the phisher who used this information to: (i) steal the customer's identity for personal use, (ii) pretend to be the real customer and gamble on his or her behalf, (iii) cheat the customer of any money or playing credits, and (iv) resell the customer's information to other cybercriminals or competing gambling sites (Chen et al. 2005, p. 3; Thompson 2007; Emigh 2005).

Many lottery scams also utilized phishing tactics. While researching internet-based lottery scams for my thesis, I too was targeted by numerous scams, such as 'UK National Online Lottery', 'The National Lottery', and 'British National Lottery', between 25 to 30 times. For instance, I first received the following email:

> Pin No:9387001
> Dear Winner,
> Winning Notification
> This is to notify you that you have won £850,000.00 in the Uk National Online Email Lottery held on 27th Dec. 2007 in Uk, e-mail addresses are picked randomly by computerised balloting powered by the Internet. Your email address was amongst those chosen for this period.
> Ticket no: 56475600545 188
> Serial no: 5368/02
> Winning number: 05.14.22.25.36.05 {06}
> Draw (#1187)
> To claim your prize, please contact:
> Fiduciary Agent Mr.Brian Adams
> Email: winner@thenationaloffice.org
> Tel: +447031945687
> Yours faithfully,
> Dr. Lorraine M. Dodds

I had never visited the UK National Online Email Lottery website, or purchased a ticket, or even entered my email address for any lottery draw. Even though I had not responded to this e-mail, I was bombarded for the next two to three weeks with a series of emails, such as:

> WINNING NOTIFICATION:
>
> We happily announce to you the draw (1155) of the U.K NATIONAL LOTTERY, online Sweepstakes International program. Your e-mail address"Attached to ticket number:"56475600545188" with Serial number" 5368/02" drew the lucky numbers: 12. 17. 21. 25. 31. 37. [30] Bonus Ball which subsequently won you the lottery in the 1st category i.e. match 5. You have therefore been approved to claim a total sum of £4,000.000.00 (Four Million Pounds Sterling) in cash credited to file "KTU/9023118308/03." This is from a total cash prize of £12,000,000" shared amongst the (3) lucky winners in this category i.e. Match 5 plus bonus. All participants for the online version were selected randomly from World Wide Web sites through computer draw system and extracted from over "100,000" unions, associations, and corporate bodies that are listed online. This promotion takes place weekly. To file for your Claim; please contact our fiduciary agent. Catherine Nola (Mrs.)
>
> Email: nola107@jmail.co.za
>
> Sincerely,
> U.K NATIONAL LOTTERY Member Services
> Sweepstakes International Program.
> NORRIS WARNER.
>
> Warning! Fraudulent emails are circulating that appears to be using National Lottery addresses, but are not from The National Lottery. PLEASE REPORT IMMEDIATELY.
>
>

Interestingly, there were several discrepancies between the two e-mails, which further indicated the fraudulent nature of this operation. First, though the 'ticket numbers' were the same in both emails, I had 'won' different amounts (£850,000 vs. £4,000,000). Second, though the ticket numbers were the same, the winning numbers drawn were

different (05.14.22.25.36.05 {06} vs. 12. 17. 21. 25. 31. 37. [30]). Third, the fiduciary agent 'Mrs. Nola's that I had to contact to claim my prize was located in South Africa (as indicated by her email address nola107@jmail.co.za), which was odd for a British lottery. Furthermore, this lottery scam warned its victims of fraudulent emails that used National Lottery addresses, which added an air of legitimacy to its illegitimate operation. Though I did not respond to these scams, several individuals were often duped.

When a victim contacted the sender of the email, "successive expenses [were] asked of him before the payment of the non-existent prize. Certain victims [suffered] losses worth several hundred thousands of Euros", and this 'industry' generated turnovers of several billion dollars per year (CERT-LEXSI 2006, p. 12). Consider the case of Sean Pearcy who received an email in early October from 'Lucky 7 Lottery' notifying him of his $2.7 million jackpot winnings. He was then asked to email a lottery official named 'David Thomas' with a 16-digit reference number he had received in the email. When Pearcy emailed, Thomas replied "To qualify for your prize money, you are expected to fill our prize winning claims form B0-7" using a web link (Barrett 2004, p. 1). Pearcy clicked on this link, and was redirected to an online questionnaire that asked for his home address, phone number, employment information, and even included a "box to check if he wished to give a press conference" (Barrett 2004, p. 1). After filling out this 'claims form', Pearcy received a string of emails from a larger number and "ever more foreign-sounding, cast of characters – 'Mr. Ndoulou Granger' in South Africa, 'Ms. Blanc Fernandez' in Monaco – each asking him to verify some bit of information" (Barrett 2004, pp. 1-2). By mid-October, Pearcy received further communication from the 'Unie De Banque Monaco', titled 'PAYMENT ORDER ENDORSEMENT NO TZ72201049',

which instructed him to get the transaction notarized. As this was a foreign lottery, the Lucky 7 lottery officials had hired the barrister 'Petts Richard and Associates' in South Africa to assist him with this task. This was followed by another e-mail asking for Pearcy's scanned copies of his driver's license or passport and a "check for $2,170 as a legal and administrative cost" (Barrett 2004, p. 2). Pearcy became suspicious and investigated who owned the lucky-7lotto.net website; records indicated a California address and phone number (Barrett 2004, p. 2).

Also consider the case of the Massachusetts State Lottery site that was cloned to trick customers. Massachusetts State Lottery Officials and the FBI shut down two fraudulent sites that mimicked the official Massachusetts State Lottery site, www.masslottery.com (Walters 2003, p. 10; Rosencrance 2003, p. 1). Cybercriminals spoofed the official website twice: once as www.mass-lottery.org and again as www.mass-lotto.org, in order to steal personal and financial information from customers throughout the US (Rosencrance 2003, p. 1). The fake lottery site was identical to the official site and even included an image of the state treasurer. The cybercriminals then used phishing attacks to contact more than 200 individuals worldwide via emails informing them that they had won cash prizes. Victims were given userIDs and passwords to log into the fake sites, and were asked to provide their financial information so that these non-existent winnings could be received. When victims clicked on links in these emails, they were taken to the spoofed website, logged in, and asked to supply personal information, such as credit card numbers, social security numbers, and processing fees (Rosencrance 2003, p. 1; Walters 2003, p. 10).

Conclusion

This chapter examines an assortment of criminal techniques that cybercriminals employ to commit crimes at gambling sites. It demonstrates how certain techniques require greater expertise than others. For instance, creating rootkits, manipulating gambling software, and generating cloned websites necessitates high levels of technical knowledge; however, cybercriminals employing toolkits and automated bots do not require the technological know-how in order to commit crimes. Thus, digital techniques vary with respect to the requirement for technical expertise, and so I ask: How does the absence of technological knowledge determine criminal organization? Can cybercriminals use toolkits and bots to operate successfully alone? Furthermore, the data illustrates how cybercrimes vary with respect to their organizational dynamics. For example, some techniques, such as using automated bots and intercepting data flows, are rudimentary in their organization; individual cybercriminals conduct these acts with little planning or coordination. Other events, however, such as assembling a botnet army require intricate preparation, scheduling, and sophistication. In light of the range of organizational dynamics, I ask: Are specific techniques used by certain types of cybercriminals? Does the sophistication of the technique determine criminal organization? Do cybercriminals use techniques to create small-scale partnerships or larger criminal enterprises? Finally, criminal techniques are used individually or in combination to create multiple, unique, and sophisticated attack possibilities that are difficult to track. For instance, cyberextortion requires several techniques, such as creating and disseminating viruses to infect machines, assembling and instructing the botnet army to attack gambling sites, and obtaining and wiring extortion payments into

offshore accounts. This interconnection of techniques not only suggests a complex organization of criminal technique, but also of criminals, and so I ask: How does the marriage of technical skills and expertise shape criminal organization? What other factors impact criminal organization? The questions raised in this chapter are addressed next, where I examine how different online criminal organizations use the abovementioned techniques to commit a variety of crimes at gambling sites.

Chapter 5

Organizing Cybercrimes

Introduction

Cybercriminals often organize themselves around the types of crime they commit, which involves different alliances, expertise, and division of labour. This chapter presents my findings on the different criminal organizations seen at gambling sites to illustrate how the type of cybercrime, digitized criminal techniques, and hacking cultures collectively impact the organization of cybercriminals. The first section examines the simplest form of online criminal organization – techno-nomads. It details the different types of techno-nomads, the range of their proficiency, and reasons for successful solo operations. The second section examines the next level of criminal organization, where techno-nomads work together as digital associates. I discuss the need for alliances between cybercriminals to engage in collusion, fraud, and criminal businesses, each of which is illustrated with examples from the online gambling context. In section three, I examine the most complex criminal organization, namely the striated assemblage, which involves organized crime groups, digital associates, and techo-nomads. This section describes how criminal networks are organized for committing crimes of cyberextortion, identity theft, online lottery scams, and fraud. For each type of criminal organization, I also discuss the motivations and rationales of cybercriminals, their communication and culture, as well as the organizational means used to circumvent external threats where applicable.

Techno-nomads

Hackers often engaged in solo operations. These techno-nomads attacked victims, not by summoning the combined efforts of ten or twenty hackers, but by using technology, and automated techniques that enabled them to bypass digital defenses. As Brenner (2002) observed, "strength [was] in software [and programming expertise], not in numbers of individuals" (p. 27). Techno-nomads were analogous to soldiers; they planned and executed attacks with precision and guile, gathering information on weaknesses in gambling sites and software (McGeathy 2001, p. 123). Hackers were technology savants who possessed technical knowledge and programming skills that compromised systems, stole or modified data, and manipulated software for their criminal interests. As discussed in the previous chapter, they used techniques such as phishing, manipulating site servers, intercepting data flows, and deploying malware. Techno-nomads operated alone for two reasons: (i) the minimal risk of detection, and (ii) the inadequacy of security measures.

The minimal risk of detection and apprehension permitted cybercriminals to operate alone successfully. Unlike traditional land-based gambling, such as state-run lotteries or casinos, which were highly regulated by the government, online gambling was subjected to limited regulation as betting sites were often located offshore and therefore beyond the reach of regulators (Kish 1999, p. 453; Keller 1999, p. 1592). Thus, regulators could not always ensure fair games and online gamblers did not know whether they were playing legitimate games (Kish 1999, p. 453; Keller 1999, p. 1592). Furthermore, when fraud victims contacted law enforcement authorities, they were told that little could be done as these companies existed in jurisdictions beyond their reach (Zacharias 2004, p. 4;

Penenberg 1998, p. 1). Thus, cybercriminals did not need a confederate to serve as a lookout for external threats.

Gambling sites also had restricted security measures that hackers easily exploited on their own. Hackers observed that companies did not concern themselves with security fixes even after approaching them about system vulnerabilities: "I would tell them how to break in, and how to fix the problems. I'd give them advice and they would never follow it. Three weeks later I would go in and I still had access to their computers" (PBS 2001b, p. 3). One gambling consultant stated "there are a number of groups trying to make money by hacking... Where would you go? I'd go to dodgy online casinos" (Warner 2001, p. 2).

Techno-nomads varied with respect to their technical skills and motivations. The *novice* techno-nomads included hackers who were new to hacking and relied on pre-written hacking toolkits to conduct their crimes, or who possessed the technological knowledge to detect and exploit system loopholes and design flaws, but were unable or unlikely to execute specialized hack-attacks (Rogers 2005, p. 3). For instance, novice techno-nomads purchased numerous pre-packaged hacking and phishing toolkits that offered different functionalities, such as scanners, sniffers and snoopers, malware, password crackers, denial of service tools, logic bombs, and dumpster diving (Gu, Liu & Chu 2004, pp. 5-7). Thus, these toolkits not only reduced the need for technical expertise, but also the need for partnering with those who possessed more advanced technological knowledge, thereby allowing novices to operate alone successfully. For example, novices downloaded automated gambling bots, which allowed them to cheat at gambling sites. Consider again the case of PokerSmoke. The PokerSmoke testimonials demonstrated

how cheaters used poker-bots single-handedly, causing significant damage to the online poker industry. One hacker claimed: "My Earnings Have Soared From $2000 A Month To Well Over $8000!". Another stated that he "Cleared A Massive Bonus In Two Days, Netting An Amazing Profit Of $550!". A third insisted that in "Just 4 Short Weeks [he] Increased [his] Poker Bankroll By 1000%" (SmokePoker.com 2008, p. 1). While the motivation of the PokerSmoke hackers was the procurement of money, others used hacking toolkits to satisfy their thrills and egos (Rogers 2005, p. 3).

Some hackers, however, engaged in cheating practices without requiring any bots or pre-packaged toolkits; they exploited poor design flaws in the gambling site. Consider the case of 16 year old Josh 'JJProdigy' Field, who was banned from PartyPoker.com for playing on multiple accounts concurrently. JJProdigy won a $500K tournament and was set to play the next tournament of $140K; he lost, however, to another player, 'ABlackCar'. PartyPoker later discovered that Fields had operated both accounts himself and won twice, robbing PartyPoker of nearly $200K. JJProdigy exploited the inadequate security checks at PartyPoker's site: "To pull it off, it is quite simple. Sites can detect two things: ip addresses and the computer used. As long as you have different ip addresses and different computers, it is an easy stunt to pull off" (as cited in Gilad 2007, p. 1). PartyPoker.com eventually closed both accounts (Angerman 2008, p. 2).

Underage gamblers typically played for thrill and were often encouraged by their friends (Meerkamper 2006). Several gambling sites, such as Ladbrokes, had rigorous age and identity verification systems in place, where the information entered by customers was validated against the databases of credit card companies and the national electoral voting organization, which gave around 98% proof of the customer's age (Dewar 2001, p.

357). Most gambling sites, however, offered little gatekeeping; the age restrictions on these sites were often "buried away in the small print", making them difficult to locate, or age verification checks involved players simply ticking a "box to say they [were] 18 years of age or older", or entering their date of births (Smeaton & Griffiths 2004, p.50). Not surprisingly, youths easily bypassed both these primitive and *pro forma* safeguard techniques by lying about their age (Andrle 2006, p. 75; Dewar 2001, p. 357; Griffiths 2003, p. 562; Keller 1999, p. 1592; CERT-LEXSI 2006, p. 18). Furthermore, applications were often accepted before age verification was complete, which allowed minors to gamble and defeated the purpose of age verification checks. Consider the study conducted by GamCare, National Children's Home (NCH), and CitizenCard (2004), which revealed that only seven of 37 gambling sites successfully denied a 16-year-old from registering and creating an account: "the youngster from London was able to lie successfully about her age and register her details on websites...", such as www.betfair.com, www.bluesq.com, www.celebpoker.com, www.coral.co.uk, www.galacasino.co.uk, www.meccagames.com, www.paddypower.com, www.paradisepoker.com, www.punt2punt.com, www.sportingbet.com, and www.willhill.co.uk (GamCare 2004, p. 3). Furthermore, she was able to participate in several different forms of gambling using the accounts created at each site (GamCare 2004, p. 1). Clearly, applications were accepted before age verification was complete, which easily allowed minors to gamble online. Underage gamblers not only exploited these inadequate security checks, but often used their parent's personal information, identification numbers (PINs), passwords, credit cards, debit cards, and electronic monies, which enabled adolescents to successfully register and create accounts at online

gambling sites (SNJCI & AGNJ 2000, p. 108; Dewar 2001, p. 357; Kelley, Todosichuk & Azmier 2001, p. 16). The youth in the GamCare (2004) study used her "Solo card" to register at the 37 gambling sites. Of the seven sites that blocked the youth, two did so because they did not accept Solo debit cards, and not because they had proper age verification systems in place (GamCare 2004, p.3).

Insiders were techno-nomads who were either current or past employees of gambling sites that abused their access privileges inherent to their job functions to attack their own site's systems (Rogers 2005, p. 3). For instance, customer lists frequently 'disappeared' at gambling sites. In one case, an employee at BetOnSports.com hacked into the company's Human Resources database and stole its customer list (Costigan 2007, p. 1; Pregame.com 2006, p. 2). The "two dozen or so computer geeks" employed by BetOnSports regularly hacked into company databases and altered information (Pregame.com 2006, p.2). As one BetOnSports executive noted, they were "like little monkeys trying to prove how good they were with computers"; they competed with each other to demonstrate their technical expertise (Costigan 2007, p. 1). These employees got a "kick out of taunting" the company's executives (Pregame.com 2006, p. 2).

Entrepreneurial techno-nomads rented or sold their malware creations, technical services, and 'digital loot' for money. Malware and services, such as toolkits and bot-networks, were often sold to *novices* or *criminal assemblages* via underground economy servers. For example, one hacker offered spyware and malicious code for $800, which was guaranteed for six months and accompanied by customer support and upgrades during the period if the malware was detected (Jellenc & Zenz 2007, p. 42). Another offered his entire hacking toolkit, which included more than "30 exploits for Windows,

an Internet infiltration system, 10 methods for circumventing anti-virus programs, a simple injection method in C++ and [the hacker's personal] website for $8,000 US, or about $260 per exploit" (Jellenc & Zenz 2007, p. 43). Another attack tool was the 'POD 1.1', which was a "free ping of death denial of service attack tool" that offered a vast amount of exploits, hacking, and general tools (Brothersoft.com 2008, p. 1). Cybercriminals also offered their botnet services as hourly, daily, and monthly rentals to the "technical illiterates" for a range of prices – 10 bots for a 24-hour 'test-drive' cost $5 US, while renting 500 bots for one month cost $220 US (Jellenc & Zenz 2007, p. 43). Some operators rented their networks to others "for as little as $200 to $300 an hour", while other small-scale attacks cost between "$1 and $40" (Biever 2004, p. 1; McAfee 2005, p. 13). Installation and support services were included in the price and discounts were offered to potential partners (Jellenc & Zenz 2007, p. 43).

Entrepreneurial techno-nomads also sold digital loot acquired from their hack-attacks at gambling sites. These hackers used their own expertise to conduct these attacks or used toolkits developed by other entrepreneurs. 'Carders', for instance, sold illegally obtained customer information to rival gambling companies or third parties for profit and operated through newsgroups, message boards, Internet Relay Chat (IRC) channels, and websites (McMillen & Grabosky 1998; Arkin et al. 1999; Payton 2005). Shadowcrew.com, CardersMarket.com, and CarderPlanet.com websites were "the WalMart of the Underground"; their servers provided an active market where carders sold credit card numbers, expiration dates, and billing addresses in either small packages for ".40 to $5", or in bulk packages of 500-5000 credit cards at a time (McAfee 2007, p. 9; Payton 2005, p. 123; Symantec 2007b, p. 12). This information was transmitted

globally with great ease over the internet, and hackers sometimes used this illicit data to extort gambling sites by threatening to publish it or sell confidential customer information (O'Brien 2000; Payton 2005). Furthermore, these cybercriminals exchanged information through online hacking communities on how to exploit, rent, sell, and/or trade "pilfered credit and debit card numbers, hijacked bank accounts and stolen personal data", indicating a strong hacker network and support system (McAfee 2007, p. 10; Acohido, Swartz & Ward 2006, p. 1). The emergence of these underground servers as cyberstores and trading grounds for illicit information indicated the "increased professionalization and commercialization of malicious activities" (Symantec 2007b, p. 12). These crimes not only impacted customers who were the direct victims of identity theft, credit card theft, or theft of playing credits, but also online gambling sites that lost their reputations, because they had poor business practices, and could not protect the confidentiality and security of their customers. Hackers used these inadequate security measures as justifications for their acts; as one hacker noted: "there are a lot of people out there who won't even safeguard their own safety, let alone the safety of their customers. At the end of the day, it's the fault of these companies... But [the companies are] not even trying to protect their own businesses" from attacks (PBS 2001a, p.2).

Professional techno-nomads had a high degree of technical acumen, access to state of the art equipment, and used their technical expertise to further their own criminal pursuits (Rogers 2005, p. 4). Like the entrepreneurs, they were motivated by money, but they either used their skills to attack their chosen targets, or worked for organized crime groups as employees, rather than renting/selling their products in underground economy servers. In February 2008, the Shadowserver watchdog group monitored a DDoS attack

in progress (Adair 2008, p. 1). They noticed that a techno-nomad had been using botnet armies to overwhelm several gambling sites such as www.fulltiltpoker.com, www.titanpoker.com, www.cdpoker.com, www.titanpoker.com, favoritbet.com, www.marathonbet.com, www.sport-shans.com, www.intercasino.co.uk, overbetting.ru, and onlinecasinos.ru, over a span of eight days. The hacker did not target a particular gambling site, but several sites in order to disrupt their service operations; "some were attacked for a few hours and others for a few days. Each attack [was] designed to overwhelm the websites with tons of bogus [connection] requests" (Adair 2008, p. 2). One attack against Full Tilt Poker left its website inaccessible for approximately 48 hours, while another resulted in its online poker room crashing numerous times including an "embarrassing outage during the final table of the FTOPS main event" (Online-Casinos 2008, p. 1). Titan Poker's functionality was also affected; initially its site loaded intermittently and later the site was unavailable for several hours (Adair 2008, p. 2). While the Shadowserver group speculated that the hacker may have been paid by other companies to damage their rivals, more likely the attacks were 'test-runs' preceding extortion attempts, as cybercriminals often hacked into their targets' computer systems to understand their inner workings before commencing an attack (Adair 2008, p. 2; Jellenc & Zenz 2007, p. 27).

Many of these cases illustrated how techno-nomads easily operated on their own by exploiting system vulnerabilities and poor security features, possessing insider knowledge, and using sophisticated technological attacks. The hacker subculture and various online communities allowed techno-nomads to learn from each other, update their skill-set, gain the latest information on security measures and how to circumvent them,

and access hacking toolkits, which armed techno-nomads with the latest knowledge that allowed them to operate alone successfully. Furthermore, many hackers had little fear of detection as they could remain anonymous. Some cybercriminals, however, were apprehended, which suggested that solo operations were not always successful.

Digital Associates

Cybercriminals often worked together as it offered certain benefits that were not available by working alone. Cybercriminals engaged in a minimal division of labour by working together in small groups. Furthermore, these partnerships were transient in nature, allowing digital associates to come together to commit specific crimes, then disband upon its completion, once again becoming free agents to form new alliances. These dynamic partnerships were ideal arrangements for committing collusion and fraud, and for operating lucrative businesses.

Cybercriminals often colluded together; two or more players, and/or gaming operation staff, worked together to influence the outcome of an online game (Smed, Knuutila & Hakonen 2006, p. 1; AGCC 2006, p. 28). Players exploited system vulnerabilities and gaming software bugs, which denied honest players the opportunity to gamble and allowed only cheaters to win. Players either partnered with other players, non-participating experts, or spectators (kibitzers in Bridge) (Yan 2003, p. 4; Smed, Knuutila & Hakonen 2006, p. 2). Each type of partnership offered unique advantages in the collusion process. For instance, spectators revealed extra information (opponents' cards) to their colluding partners. Expert players offered advice, tips, and winning strategies. Active players conspired for their interests, such as letting the colluding partner win or swapping user accounts, and then sharing the winnings. No hierarchy or

set authority existed and players contributed equal amounts to the colluding process to ensure their goals were met. Colluders had different types of agreements; they had a prior explicit hidden agreement, had no prior agreement but worked together during the game, or had limited agreements regarding certain decisions but competed normally otherwise (Smed, Knuutila & Hakonen 2006, p. 1). Colluders decided the cheating details in these agreements, such as which cheating methods to use, how to share knowledge and information related to the current game situation, and how to receive, donate, or trade game-related resources with the each other (Smed, Knuutila & Hakonen 2006, p. 3).

These collusion agreements and partnerships gave unique characteristics to each colluding tactic. Consider the case at FullTiltPoker.com during the multi-table tournament (MTT) in 2007. Chris 'BluffMagCV' Vaughn was declared the winner and entitled to the one million dollar prize. This prize, however, was soon given to runner-up Soren Kongsgard as it was discovered that Vaughn had engaged in a colluding practice called 'seat-stealing'; he sold his seat to his friend Sorel 'Imperlum' Mizzi and was going to receive a percentage of Mizzi's prize (Angerman 2008, p. 2). Vaughn stated, "we were on instant messenger and I sent him [Mizzi] a message and, it pretty quickly led to a discussion about selling the account" (WPR 2007, p. 1). Mizzi earned his living by playing poker, and his success permitted him to pay Vaughn a "few thousand bucks at a chance to win a few hundred thousand" (WPR 2007, p. 1). Vaughn rationalized his actions by noting that other players had engaged in seat-stealing, including top players who purchased the "rights to their account while deep in a tournament" (WPR 2007, p. 1). Mizzi then logged on to Vaughn's account from home, and other contestants immediately "faced a completely different BluffMagCV, one with a different playing

style, incredible amounts of online MTT experience and over $500K in live tournament winnings" (Angerman 2008, p. 2). Vaughn and Mizzi won because they were well-coordinated. FullTiltPoker, however, tracked the account swap to Mizzi's home IP; both Vaughn and Mizzi were banned from FullTiltPoker and each was "relieved of [his] winnings" (Angerman 2008, p. 2). As one security expert noted, "if Sorel and Vaughn lived together, nobody would have known this happened. This [seat stealing] isn't going to stop, simply because it's unenforceable" (WPR 2007, p. 1).

Cybercriminals also colluded with gambling site operators or game developers, who offered inside information (Smed, Knuutila & Hakonen 2006, p. 7). Consider again the AbsolutePoker.com scandal, where Potripper and #363 colluded to deny honest customers a fair game. Investigations linked #363's IP address to a part-owner of the company, Scott Tom, and the Potripper account to a former executive of the site, AJ Ripper (Goldman 2007, p. 2). Here, the insider at AbsolutePoker.com (Tom) had real-time access to all of the 'hole cards' and relayed this information to his outside accomplice (Ripper) (Levitt 2007, p.2). In addition, six others – GrayCat, PayUp, SteamRoller, XXCashMoneyXX, DoubleDrag, and RonFaldoXXB – were 'superuser' accounts, which were deployed over a period of six weeks to read honest players' hole cards (KGC 2008, p. 1). GrayCat and DoubleDrag enjoyed substantial winnings in a short time frame. They often threw "away hands on flops despite raising preflop a lot suggesting that they were aware of when their opponents hit the flop" (Casinomeister 2007, p. 7). Another case indicating a partnership between an insider and an outside hacker was BetOnSports. In August 2006, the Argentinian sports betting firm 'Formoapuestas' owned by BetOnSports was hacked into by disgruntled customers, who

replaced the sportsbook content with the message: "BOS [BetOnSports] SUCKS PAY YOUR CUSTOMERS AND EMPLOYEES, or you will be held accountable" (Gambling.co.uk 2006, p. 3). The inclusion of customers and employees in the defacement message clearly indicated an alliance between the two, with the latter providing access to the company's servers, which made the attack possible.

Unscrupulous site operators also committed fraud against their customers in several ways: (i) withholding revenue, where site operators did not give payouts to honest customers, (ii) overcharging customers, where gambling operators claimed payment for services that were not consumed by customers, (iii) manipulating redistribution rates, where operators tampered with existing payout rates, or did not reveal the redistribution rates, (iv) providing unfair gambling odds, where gambling operators tampered with gambling applications to generate fewer winners and lower winnings, (v) stealing financial information, where site operators used customers' financial data at their own discretion without the prior knowledge of their customers, and (vi) malware propagation, where gambling-specific software contained "silent installs of adware or even malware... [which stole] bank cards and online banking information" of customers (Kvarnstrom, Lundin & Jonsson 2000, p. 8; CERT-LEXSI 2006, p. 1, p. 9; Andrle 2006, p. 75; Zacharias 2004, p. 4).

MaxLotto, an online provider of lottery services, illustrated how digital associates worked together to commit fraud. This site was created in October 2000. It advertised that approximately 10% of its revenues would be donated to Canadian charities, and used online marketing campaigns and referral systems to attract Canadian customers (Kelley, Todosichuk & Azmier 2001, p. 5). The company, however, defrauded both customers

and other charities; when the Canadian charities listed on MaxLotto's site as benefactors were contacted, few knew of the company or had received any donations from the site (Kelley, Todosichuk & Azmier 2001, p. 5). MaxLotto, as discovered later, was co-founded by Brian Tierney and Stuart Kinder, who worked together at Lehman Brothers in New York (Kelley, Todosichuk & Azmier 2001, p. 5; PRNewsWire 2001, p. 2). The site was licensed in the Dominican Republic, its servers were operated by 'Cable & Wireless', which had principal operations in the Caribbean, Panama, Macau, Monaco and the Channel Islands, and its marketing subsidiary, 'RagingHippo, Inc.', operated out of New York, which clearly indicated that the MaxLotto associates were scattered globally (Kelley, Todosichuk & Azmier 2001, p. 5; PRNewsWire 2001, p. 1). When I accessed MaxLotto.com in 2008, it did not have any content relevant to online lotteries, contact information, or online registration for potential customers. Upon further investigation, I discovered two different explanations: MaxLotto's past marketing director stated that the company was sold to a private gaming firm in 2001, while LotteryCanada.com stated that MaxLotto had shut down due to high insurance rates after 9/11; the company could no longer afford "coverage to insure a win in case they didn't have enough ticket sales for that draw" (Bortz 2008, p. 2; LotteryCanada, personal communication, April 4, 2008). Both explanations suggested that MaxLotto.com was defunct by 2002. Interestingly, the site resurfaced in 2004, was registered to 'HLK Enterprises, Inc.', and did not offer any online lottery services. MaxLotto's disappearance and reappearance demonstrated the dynamic and transient nature of this fraudulent gambling site [Figure 4].

Another example of partnership crime was the online lottery fraud that operated from India. This fraud group consisted of three known members: Nigerian Festos

Albaika, and two Indians, Harish Acharya, and Jayant Sagwekar (IndianExpress 2008, p. 1). Albaika, who was the leader of the scam, had resided in India long after the expiration of his work visa. He met Acharya, a goldsmith, when he went to Acharya's shop to purchase a gold pendant. Albaika mentioned that he wanted to transfer some friends' money to Mumbai, but was unable to do so as he was a foreign national. Acharya agreed to assist Albaika in the money transfers. Acharya served as the middleman and was responsible for convincing Sagwekar and other 'agents' to open bank accounts across Mumbai. These agents then handed over their passbooks and debit cards to Acharya, who then gave them to Albaika. Next, Albaika sent a mass-email across India congratulating numerous victims on winning an online lottery worth millions of rupees. This email instructed the 'winners' to deposit funds for service charges into the bank accounts created by the agents. These winners parted with their money, but never received any 'winnings'. Once the money was deposited, Albaika wrote a withdrawal cheque, which was encashed by Sagwekar and other agents. This money was then handed over to Acharya, who in turn gave it to Albaika. In this manner, Acharya handed approximately 80 lakh Rupees (eight million dollars) to Albaika in 2007 alone (TimesOfIndia 2008, p. 1). In return, Acharya received a 4% commission and the agents earned 3% (TimesOfIndia 2008, p. 1). At the time of the arrests, it was anticipated that more individuals were part of this fraudulent operation, suggesting that this criminal group may be larger (IndianExpress 2008, p. 1).

Like entrepreneurial techno-nomads, digital associates also offered an assortment of services for sale. As one security expert noted, some hacking groups offered "boutique virus writing services that [produced] malicious programs that security software will not spot", which illustrated their technical expertise (BBC 2007, p. 1). These groups also operated volume pricing schemes and discounts for loyal customers, demonstrating the marketing and customer service attributes of the group. These digital associates preferred selling hacking kits as this put them at minimal risk if their kits were used to commit crimes; the success of the MPack toolkit worried its creators as "it was made by a group of friends and they all [had] regular jobs" (BBC 2007, p. 2).

Another way the entrepreneurial digital associates operated was in the underground botnet economy. Recognizing that botnets were a source of substantial illegal revenue, hackers actively worked together with each other with the common goal of acquiring profits (ITU 2008, p. 13). This group of digital associates comprised malware authors, who wrote and disseminated malware, bot-herders, who controlled the botnet armies through 'command and control' channels, and clients who commissioned new malware development or botnet activity to pursue various criminal activities, such as spam, identity theft, and DDoS attacks (ITU 2008, p. 13). In spite of this group work, the botnet economy was competitive, with rival digital associates attacking and seizing each others' botnet armies, which was often cheaper and easier than designing a bot network from scratch (ITU 2008, p. 14). These digital associates communicated through heavily encrypted Internet Relay Chats (IRC), which possessed attractive qualities, such as "n-way communication and the ability to communicate in near-real time" (Kilger, Arkin & Stutzman 2004, p. 551). When a member of this botnet group left, the replacement was

extensively screened by existing members to prevent 'fraudsters' (law enforcement, security agents, or rivals) from entering the group (ITU 2008, p. 14).

The above data illustrated that digital associates were able to commit a different set of crimes (than techno-nomads) at gambling sites because of their organizational dynamics. They used regenerative techniques, such as disappearing and reappearing, to evade policing threats, formed alliances with insiders to get access to otherwise secure systems, and used dispersed memberships to avoid easy apprehension. Some cybercrimes, however, required even more sophisticated organization, extensive group membership, and elaborate divisions of labour, as discussed next.

Striated Assemblages

Organized crime groups brought their tried and true techniques from the physical realm into the virtual world (Gray 2005). As one security expert observed, online organized crime was "likely to be better funded, better skilled and better organized than lone criminals... I think organized crime is a big worry, and I think it's going to get worse" (PBS 2001c, p. 3). Online organized crime networks extended over space and time using ICTs. They required "less personal contacts and thus less relationships based on trust and enforcement of discipline between criminals" (Council of Europe 2004, p. 9). Hierarchical structures were often not needed to carry out organized crime attacks on the internet. In fact, ICTs favoured those organizations that were already based on flat-structured networking, with "loose collaborative criminal [sub-] networks" (Council of Europe 2004, p. 9; McAfee 2005, p. 10; CCRC 2005, p. 1). Each sub-network worked together to successfully implement cybercrimes.

Organized crime groups often extorted gambling sites. Cyberextortion was defined as a "sophisticated threat, combining computer intrusion, theft, destruction, and modification of data, social engineering, and fear instilled in victims by threats from would-be extortionists" (Bednarski 2004, p. 1). Cyberextortion rings had a complex division of labour and comprised smaller sub-networks that specialized in particular tasks, resulting in a horizontal division of responsibility [Figure 5]. Many of the roles identified earlier in Lemieux's (2003) crime network were evident in these cyberextortion rings. These groups involved 'organizers' who arranged plans to be executed by other sub-networks in the criminal enterprise. They were of two types. 'Hybrid' organizers had shifted from traditional forms of hacking to create organized crime groups that exploited new online opportunities (Gray 2005, p. 1; Germain 2004, p. 1). Indeed, the mastermind in one cyberextortion ring was a 21-year-old Russian mechanical engineering student who studied computer programming and website design before hacking gambling sites for a living (MIL 2000, pp. 1-2; CCRC 2005, p. 2). Another cyberextortion ring comprised "well-educated [organizers] in their early 20s" who met online and agreed to work together; there was "no chief organizer in plain terms, each of them did his bit of work" (Isachenkov 2004, p. 2). 'Hired' organizers were technologically savvy individuals who carried out online attacks at the behest of international crime syndicates, such as the Mafia, Latin American, Middle Eastern, Eastern European, and Asian crime groups (Germain 2004, p. 13; McMullan & Rege 2007, p. 655; Williams 2002, p. 10). These crime syndicates provided the required capital to finance extortion attacks. For example, computer hackers associated with the Russian mafia extorted Worldplay System, and several casino sites until their ransoms of $50,000 were met (Walker 2004, p. 2).

'Extenders' expanded the scope of their enterprise by recruiting new members that broadened the skill sets required by the criminal network. This unit was responsible for filling vacant positions in the criminal network and creating new units, which ensured that the cyberextortion ring flourished. One network recruited college educated hackers and used 'internet advertisements' to obtain and convey the latest skills. Another ran hacking sites which schooled recruits on"150 ways to break into websites and technology systems" (Walker, 2004, p. 6). Extenders typically hired professional techno-nomads or digital associates (the 'executors' of the criminal network) as required, and found them in hacker communities and underground economy servers. For instance, the extenders of these cyberextortion rings were often involved in all stages of the botnet economy, from hiring cybercriminals to write malware to launching botnets to attack gambling sites (ITU 2008, p. 14). One ex-hacker stated that he was "contacted by a couple of different criminal organizations that offered him quite a bit of money. Other associates of [his had] been contacted by various" organized crime groups (PBS 2001d, p. 3). As one law enforcement agent stated, "it used to be naughty boys [committing cybercrimes] ... But now they've grown up. They realise if you are clever at something then [they] should use it to earn a living." (ZDNet 2005, p. 1).

Executors possessed knowledge of the inner workings of computers and network systems, algorithmic computing, reverse engineering, virus installations, program codes, and exploiting system vulnerabilities. Consider again the case of Grafix Softech. Russian hackers bypassed Grafix's firewalls and other security systems and then hacked into five servers used for the company's online operations (Glavan 2003, p. 1). Four of the servers supported several gambling sites and one contained all operational data (Glavan 2003, p.

1). The hackers then installed a virus on each server, which encrypted its sensitive information. As one security expert noted, "Grafix had state-of-the-art security. These hackers were ingenious" (Glavan 2003, p. 1). Other executors grouped together into sub-networks to execute DDoS attacks against gambling sites. For instance, one cyberextortion ring had members in Moscow, St. Petersberg, and Saratov who had never physically met. As one law enforcement officer noted, this ring was "not a normal organization. Everyone sat at home, and everyone had their role" (Bullough 2004, p. 2). Still others created malware and monitored the gambling industry's reactions and remedies to attacks so as to adapt subsequent versions of their malware for future attacks (Reuters 2001, p. 2; Warner 2001, p. 1; Swartz 2004, p. 4). For instance, the SoBig virus, which was used by hackers to compromise computers in DDoS attacks, had matured to such an extent that it was beyond the ability of an individual hacker to program (Germain 2003, p. 3). This malware was developed by a group of virus writers, who did not leave any traces of their identities in their code (Thompson 2004, p. 9). Six versions of SoBig were released throughout 2003. Each version of the worm suggested that its writers had altered it after observing "its behavior in the wild, then killing [it] off ... to prepare a new and more insidious version" (Thompson 2004, p. 9). The last variant, Sobig.F was programmed to install a back door that would allow the author to assume control of the victim's computer, making it ideal for DDoS attacks. Interestingly, the creators of SoBig 'disappeared' after learning that the "F.B.I. [was] out for the SoBig [writers] with both claws" and that Microsoft put a "quarter-of-a-million-dollar bounty on the heads of the virus writers" (Thompson 2004, p. 9; Gaudin 2004, p. 2).

Cyberextortion networks, however, did not have formal roles for insulators or guardians who typically protected the internal structure and external order of extortion networks from exposures, defections and betrayals (McMullan & Rege 2007, p. 655). Extortion rings also did not have formal positions for communicators or monitors who managed information flows between members or sub-networks within the enterprises and handled problems of internal network security and external law enforcement. These roles were either performed by existing organizers or extenders, or were nonexistent because the rarity of stable long term criminal memberships and low chances of detection made these roles unnecessary (Brenner 2002, p 50; Lemieux 2003, p14).

Cyberextortionists got their money sent in multiple broken Western Union payments, which were finally picked up by money mules (McMullan & Rege 2007, p. 658). For example, in a rare 'sting' operation, British police arrested ten suspects and charged them with collecting extortion payments from gambling sites. Once funds were brought into the extortion network, money movers deposited it into an account where it was wired around the world. The funds "bounced around [worldwide through untraceable financial networks] and eventually became impossible to trace" (as cited in Cassavoy 2005, p. 1; Germain 2004, p. 2). Crossovers provided confidential company information to cyberextortion networks about the inner workings of gambling sites, software flaws, and bugs. This information made virtual attacks easier to plan and execute for organized crime groups. In the CryptoLogic case, an employee sold company secrets to hackers, which included a sophisticated algorithmic program for deciphering RNGs. The criminal network then cracked CryptoLogic's systems disrupting its functionality (Reuters 2001). While each sub-unit in the cyberextortion ring operated in isolation, units communicated

with each other regarding the overall operation of the criminal enterprise. For instance, organizers and extenders had to communicate effectively to maintain and expand the network, but organizers may not have known the recruiting process, the avenues of recruitment, and the new hires; this separation ensured that the anatomy and operations of each unit remained unknown to other sub-networks in the cyberextortion ring. This inter-sub-network information exchange resulted in a strong overall communication system, ensuring the smooth functioning of the cyberextortion ring.

Striated assemblages were also involved in identity theft. Consider the case of Lanre Elekede, a member of an identity theft ring that hacked into BetOnSports.com. Elekede and his partners cracked the site's database and stole approximately 175 customers' personal information, such as names, addresses, phone numbers, dates of birth, social security numbers, and mother's maiden names, as well as credit card and bank account numbers (DOJ 2007, p. 1). This information was used by Elekede to make several illegal online purchases. He also shared this information with other members of the identity theft ring via email (Mark 2007, p. 1). Elekede used two email addresses, 'getting2k@yahoo.com' and 'getting2k@hotmail.com' to frequently communicate with ring members, where they exchanged customers' credit card information (which they referred to as "ikes"), personal information ("infos"), social security numbers ("sola sola"), and mother's maiden name ("mama name") (DOJ 2007, p. 1; USASDNY 2006, p. 1). Though this information was exchanged via email, Elekede kept hard copies of this information; law enforcement officials found notebooks containing victims' confidential personal and financial details, as well as the contact information for Elekede's associates (DOJ 2007, p. 1). Furthermore, the crime ring circulated several copies of the

BetOnSports customer database in underground markets to other cybercriminals and rival sportsbooks (Caray 2006, p. 5).

Organized crime networks also perpetrated frauds, which involved swindling customers via spam emails and luring them into lottery-like schemes. These scams were structured as traditional 'Nigerian' scams. First email addresses were harvested from large mailing lists. As one security expert noted, these scams displayed organized crime elements, with a "tendency to exchange 'sucker lists' and information between these 'boiler rooms'" (Barrett 2004, p. 3). Mass emails were sent out to individuals, which promised extraordinary rewards from winning fictitious lotteries. To claim these winnings, however, victims often had to given out personal information, financial details, and pay 'service fees'. The victim was typically targeted via a sequence of emails. Consider the case of Euromillion Espana. The majority of their scams were usually headed by organized crime groups, who were located in Spain, France, Australia, the Netherlands, the United Kingdom, Romania, and East Africa. These groups were large-scale, typically involving several hundreds of individuals who specialized in using traditional scam techniques via ICTs. The Euromillion Espana group was well organized and had an extensive division of labour. Some members specialized in social engineering and sent emails to their victims posing as a representative of the lottery company (CERT-LEXSI 2006, p. 13; Barrett 2004, p.3). Others created fake sites for the 'ghost' company and generated false administrative documents [Figure 6]. The official Spanish lottery elGordo.com noted that large groups of criminals of various nationalities used its name to dupe victims. These criminal groups moved with "ease around the whole world and used mobile telephones, PO Boxes, provisional or false addresses (including real addresses of

official Spanish organizations)" (elGordo.com 2008, p. 1). Furthermore, these crime networks were regenerative in nature. For instance, in 2005 Spanish police arrested 300 individuals, who operated a $200 million global online lottery scam. This void was almost immediately filled by new scam artists (Queen 2007, p. 1).

Some gambling companies committed fraud against their customers and licensees. One such criminal assemblage was that of Starnet Communications International Inc., a gambling company that participated in several different forms of fraud. Company employees engaged in 'straight stealing' to cheat its licensees of 85% of net sales. Starnet site operators tampered with customer information to create several records for the same clients. Then, they created 'fake' winners with modified betting histories; for instance, site operators would change a $ 20 win for a $ 20,000 win and the licensee was deprived of $ 19,980. The accounting unit of the company then paid the 'winner', thereby defrauding the licensee and other players of legitimate winnings (Gambling Magazine 1999, p. 1). This example illustrated that Starnet had several members who were involved in an elaborate scam. Each unit specialized in committing different tasks, resulting in a horizontal division of responsibility. The core members of the fraud group were in positions of trust; Starnet CEOs, accountants, and employees planned illegal activities, tampered with company records, and modified player betting histories respectively (Gambling Magazine 1999, p. 1). Thus, being in positions of trust, gave various Starnet employees the necessary access and opportunity to successfully commit fraud.

Organized criminal organizations often created complicit gambling sites to further their criminal pursuits. Cybercriminal groups managed several online casinos concurrently, and also operated non-gambling sites, such as "traffxxl.biz and repon.info",

which produced and disseminated malware, and "nextlittle.com", which distributed child pornography (CERT-LEXSI 2006, p. 8). Indeed, over forty active Russian-speaking cybercriminal groups, such as "Yambo, Polyakove, or Kuvayev", controlled more than a thousand gambling sites from Montreal, Boston, and Moscow, which, in turn, enabled money laundering and malware dissemination (CERT-LEXSI 2006, p. 8). The Giordano money laundering group was a case in point. The tightly-knit group involved Primary Development, Inc. and Digital Solutions, S.A., who were 'executors' responsible for developing the website www.playwithal.com, and providing servers, data and software for the sole purpose of facilitating criminal operations. Though the site was hosted in Florida, its servers were situated in Costa Rica, which had weak regulatory laws, minimal supervision powers, and weak law enforcement practices. Furthermore, start-up costs for establishing these sites were low, which also made this venue attractive; gaming licenses in Costa Rica cost approximately $10,000, required a three-month wait period, and offered anonymity for the owners (CERT-LEXSI 2006, p. 14). Despite the online gambling site, much of Giordano's enterprise still operated as a traditional illicit bookmaking business. Giordano himself controlled and oversaw the entire operation of the network, thereby acting as the 'organizer'. Giordano's son-in-law acted as the 'controller' and was responsible for overseeing the everyday operations, managing bettor account information, and handling accounting discrepancies. Giordano's wife and daughter acted as 'financial officers' and were involved in laundering gambling proceeds to offshore financial accounts. Five other individuals acted as the 'clerks', 'agents/runners', 'distributors', and 'accountants' by exchanging, distributing, delivering, and transferring gambling proceeds between members of the crime group. These sub-

networks functioned together to launder financial proceeds, and conceal the nature, location, and source of these transfers from law enforcement (NorthCountryGazette 2006, p. 3-4; GAO 2002, p. 36; CERT-LEXSI 2006, p. 1; 15). Like traditional organized crime groups, the Giordano group even had 'enforcers', who were a "team of goons on call to collect bets"; one California customer who was late in paying a $130,000 debt was told that "two enforcers were on their way to ... slice [his] face" (Venezia, Martinez & Livingston 2006, p. 2).

Also consider the networks of the Uvari Bookmaking Group [Figure 7]. The charges in the indictment against the Uvari Group included operating an illegal gambling business, money laundering, and wire fraud (USASDNY 2005, p. 2). This illegal bookmaking network was run by Gerald Uvari, his brother Cesare Uvari, and his son Anthony Uvari. This gambling ring traversed the states of New York, New Jersey, Florida, Nevada, North Dakota, New Hampshire, and Oklahoma, as well as offshore locations, such as Euro Off-Track in the Isle of Man, International Racing Group, Inc., and Elite Turf Club in Curacao, indicating a geographically dispersed membership. The Uvari Group acted as an intermediary between individual gamblers and various horseracing and sports betting companies. The group received money for each bet placed, regardless of the result, via a pre-negotiated commission with each bettor; this 'commission' was determined by the group based on the "number of accounts that the Uvari Group opened at the [offshore site], and [the commission] represented a percentage of the bet the [group] received" regardless of the bet's outcome (USASDNY 2005, p. 4). Furthermore, for each bet, the group returned a portion of its commission to the bettor, as an incentive for the bettor to remain loyal and place bets through the Uvari bookmaking

scheme (USASDNY 2005, p. 5). Thus, the Uvari group acted as a business with betting protocols and offered its customers illegal betting 'services', as well as customer appreciation through 'loyalty schemes'. The Uvari group created customer accounts for individual bettors with offshore betting sites, for which they had passwords and other details. The personal information of these bettors, however, was never associated with these accounts; instead "each account was attached to a Social Security number of one of the organizers of the Uvari Group scheme", namely the three Uvaris, Marvin Meyerowitz, and David Appelbaum. This arrangement permitted the individual bettors to remain anonymous and avoid paying any taxes on their winnings and also allowed the Uvari Group to claim income tax deductions by associating the losses of their customers with their own accounts (CERT-LEXSI 2006, p. 10).

These case studies illustrated how criminal assemblages organized at gambling sites to commit extortion, fraud, and money laundering. They ensured their prolonged success in several ways by: fine-turning subsequent attacks based on industry reactions, expediently filling compromised nodes, using insider information, and using traditional techniques, such as social engineering to lure victims and enforcers to handle uncooperating customers. The abovementioned crimes demonstrated how each type of criminal organization was able to engage in different sets of crimes. It also illustrates how criminals worked in isolation or together by exchanging information and forming alliances in cyberspace.

Conclusion

The data discussed in this chapter helped shed light on the three different types of cybercriminal organizations and how each was useful for executing different crimes at gambling sites. It demonstrated how ICTs influenced criminal organization, communication, and operation. Not only did techno-nomads, digital associates, and striated assemblages have different levels of technical expertise, but this trait varied within each typology; for instance, some techno-nomads were technologically savvy and conducted hack-attacks themselves or offered their services for hire, while others purchased toolkits and bots, which required little technical know-how to commit cybercrimes. Furthermore, digital associations and striated assemblages included members with computer expertise as well as knowledge of traditional techniques, suggesting that criminal organizations engaged in a division of labour that included a mix of old and new criminal techniques. This chapter also illustrated the complexity of the links between the organization of criminal techniques and the organization of criminals in cyberspace. Interestingly, however, the sophistication of the criminal organization was not always directly proportional to the sophistication of the criminal technique. For example, some techno-nomads working alone conducted sophisticated attacks, such as the hacker who executed DDoS attacks against multiple gambling sites. Similarly, striated assemblages did not always employ complex digital attacks. While cyberextortion rings did implement DDoS attacks against gambling sites, other criminal assemblages such as Starnet and the identity theft ring targeting BetOnSports.com, used simpler techniques of manipulation; the former tampered with customers' betting histories, while the latter hacked into and stole BetOnSports' customer database. These

cases showed that any criminal organization used a range of criminal techniques regardless of its sophistication.

In light of the above information, I ask: are all components of online criminal organization, such as social bonds and skill-sets, technological? Are traditional criminal characteristics evident in online crime? Does my integrated theory adequately capture the organizational dynamics of online crime and criminality? These questions are investigated in the next chapter, where I revisit my theoretical framework to evaluate its applicability to online criminal organization, operation, and communication.

Chapter 6

Back to Theory

Introduction

I have argued that cyberspace offers a new niche for criminals, altering conventional notions of criminal organization and operation. My study has shown that cybercrimes at gambling sites are complex phenomena comprising an assortment of digital techniques and diverse organizational dynamics. The preceding data chapters have revealed the characteristics of several criminal techniques, such as availability, frequency, duration, and sophistication, as well as the properties of cybercriminal organization, such as division of labour, redundancy, nature of ties, membership, and tactics used to circumvent external threats. The data, however, has also raised questions about my integrated theoretical framework developed in chapter two.

This chapter analyzes and interprets the data collected to assess the adequacy of my integrated theoretical framework. I organize this chapter along six dimensions. First, I summarize my integrated theory by highlighting its main characteristics. Second, I address how my integrated theory is supported with respect to cybercriminal organization, operation, and communication, by using the data from preceding chapters. Third, I demonstrate how the data falls outside the scope of my integrated framework. Fourth, I use these shortcomings to revise the concepts of space, time, and criminal structure, so that my integrated theory can account for the organizational aspects of cybercrime and cybercriminals. Fifth, I discuss how these concepts inform my integrated theoretical framework in terms of four major criteria: scope, coherence, causality, and predictive power. Finally, I conclude by outlining four areas for future research.

Theory Summarized

In chapter two, I developed an integrated theoretical framework that combined criminal organizational typologies with cyberspace theories which allowed me to develop six 'points of intersection', or dimensions, that impacted the organization and operation of cybercriminals. The first dimension, you may recall, was *scope*. I argued that cybercriminals worldwide could connect with each other at any node/site in cyberspace which, in turn, extended the scope of their interaction capacities, partnerships, and skill-sets. I also claimed that cybercrimes could be committed at and from any node in networked digital environments in any sequence; this endless permutation of connections, I insisted, expanded the reach of cybercriminals and the scope of their criminal activity. *Time* was a second dimension that I claimed influenced the organizational aspects of cybercriminals and their attacks. Cybercriminals could coalesce for limited time periods, which led to transient organizations that were frequently and easily formed, dissolved, and reformed. Additionally, cybercrimes could be committed intensely/intermittently, synchronously/asynchronously, sequentially/concurrently, and in real/chosen time for short/long time frames, which made criminal activity transient and pliable. The third dimension I theorized was *structure*. Online criminal assemblages were decalcomanic (lacked structure), decentered, and exhibited a mostly lateral division of responsibility. Furthermore, cybercrimes were implemented as assemblages that interconnected an assortment of digital techniques, such as spam emails, malware, and cloned sites. The fourth dimension I included was *movement*; cybercriminals experienced fluid nomadic movement by sporadically traversing multiple flight lines in cyberspace, which made their organizational patterns unpredictable and unknown. Digitized criminal techniques

(deterritorialization movements) were conducted by 'hopping' along multiple flight lines, which avoided creating attack patterns and made detection difficult. *Space* was the fifth dimension in my integrated framework. Cybercriminals operated in rhizomatic spaces, which facilitated networking and information exchange along several flight lines. Cybercriminals used several deterritorialization movements, such as viruses and Trojans, in rhizomatic space to 'break' striated spaces, such as secure gambling sites. The sixth dimension I presented was *preservation.* Threats of reterritorialization (cybercrime prevention and control measures) were managed using regenerative tactics; cybercriminals avoided, evaded, or neutralized disruptions via new flight lines. Cybercrimes could be persistent by continually using spontaneously created flight lines, or by continuously modifying deterritorialization movements to stay ahead of reterritorialization threats. These six dimensions formed my integrated theory, allowing me to depart from traditional ways of thinking about criminal organization and operation. I used the data collected in the preceding chapters to evaluate the strengths and limitations of my integrated theory.

Theory Supported

To start, my integrated theoretical framework explained the *online* components of criminal organizations and operations rather well. The spatial and temporal constraints experienced in physical space were overcome in cyberspace; each of the six dimensions of my theory were evident in the data, confirming that online criminal activity and organization was dynamic, ephemeral, adaptable, and suitable for cybercriminal events. Cyberspace effectively transformed criminal activity possibilities. As Brenner (2002), Wall (2007), and I argued in chapter two of my thesis, ICTs and cyberspace increased the

scope of criminal activity by expanding sites/nodes of victimization and perpetration. For instance, numerous users worldwide (nodes of victimization) unknowingly downloaded malicious software from Gambling Federation's website (single node of perpetration), which prevented many users from playing at rival gambling sites (nodes of victimization). Alternatively, numerous sites of perpetration victimized a local node, as was evident with global bots used in DDoS attacks against a particular gambling site, such as BetCris, MultiBet, Canbet, and Grafix. The smooth space of cyberspace permitted some hackers to attack gambling sites indirectly via botnet armies, while other cybercriminals targeted their victims directly, such as the hackers who rigged the CryptoLogic software, continuously allowing customers to win. Indeed, the possibilities of endless connections gave cybercriminals greater flexibility in targeting any node in cyberspace. The scope of criminal communication also increased in cyberspace, allowing techno-nomads to access several nodes of information dissemination and exchange. For instance, underground servers distributed pre-packaged toolkits, how-to-do-it manuals, and automated bots to novice hackers and cheaters. Techno-nomads accessed these nodes, which armed them with the latest information, tips, and tricks, thereby allowing them to increase the scope of their criminal activity; they cheated, exploited, manipulated, and hacked gambling sites with regularity, success, and little chance of detection. Digital environments also impacted the scope of criminal organization. As I suggested in chapter two, globally scattered cybercriminals worked together in online environments as digital associates and striated networks. For instance, while the associates involved in the MaxLotto case were dispersed across New York and the Dominican Republic, they operated together in cyberspace to create the fraudulent lotto

site. The BetOnSports.com defacement case demonstrated that some associations were formed with insiders; company employees united with disgruntled customers to attack the sports betting site. Similarly, the scope of membership in striated assemblages grew in cyberspace. Members of cyberextortion rings were often dispersed, with some executors connecting to cyberspace from ports in Moscow, St. Petersberg, and Saratov. The extenders of these rings frequented and deployed nodes of information exchange, such as hacking communities and underground economy servers, to recruit skilled techno-nomads or digital associates. Thus, unlike conventional colleagues and organized crime groups who were restricted by physical spaces in terms of their alliances and memberships, ICTs and cyberspace broadened the scope of these properties for online criminal organizations.

Time was also a flexible entity in cyberspace. Techno-nomads, digital associates, and striated assemblages often and easily manipulated time to commit cybercrimes synchronously in real time, or asynchronously in chosen-time. For instance, DDoS attacks were synchronous; several botnets concurrently flooded gambling sites with fake traffic. Alternatively, the Gambling Federation Trojan prevented customers from accessing competing gambling sites at different times, which demonstrated that cybercrimes were asynchronous. Finally, the OKBridge.com case revealed that information packets containing confidential player card details were intercepted by cheaters in real-time. Thus, online crimes were executed at the cybercriminal's behest. As my integrated theory stated, cybercrimes also fluctuated in their frequency, duration, and sequence, which was illustrated by the Shadowserver's account of the DDoS attacks against several gambling sites. In this case, a techno-nomad attacked FullTiltPoker.com

continuously and intensely for a few hours, while others, such as TitanPoker.com, were targeted intermittently for days. Criminal techniques also had diverse and varying life-spans. As the botnet economy data showed, botnets were active for approximately a month, during which they conducted one attack per day at the hacker's discretion. Some gambling sites had fluctuating life-spans; for instance, MaxLotto.com operated between 2000 and 2002, then disappeared in 2003 only to reemerge a year later in 2004. Other fraudulent and shell gambling sites, such as GlobalSportsNet; Fallons, BingoWorld, Mass-lottery.org, and Mass-lotto.org disappeared entirely after they were discovered and deemed fraudulent. Indeed, cybercrimes varied with respect to their timing, duration, frequency, and life-span, clearly indicating the malleability of time in cyberspace. As I argued in chapter two of my thesis, cybercriminals interacted in both chosen-time and real-time, which was demonstrated by the communication techniques used by the identity theft ring that stole customer data from BetOnSports.com servers. Here, cybercriminals communicated with each other via emails in chosen-time, while they sold the stolen data to other hackers in underground economy servers in real-time. The underground botnet economy used IRC mediums, which allowed several cybercriminals to interact concurrently in real-time. Vaughn and Mizzi, for example, communicated in real-time over instant messenger while cheating at FullTiltPoker.com. Similarly, in the AbsolutePoker.com case, #363 had real-time access to everyone's hole cards, and relayed this information back to his associate Potripper instantaneously. Finally, as my integrated theory suggested, the life-span of criminal organizations also varied; bonds between members were transient and the organization lasted for short time frames. As Vaughn and Mizzi's antics aptly demonstrated, cybercriminals came together for limited time periods

during FullTiltPoker's MTT tournament, committed specific crimes, such as seat-stealing to win tournaments, and quickly departed after the criminal event. Similarly, the extenders in some cyberextortion rings recruited executors to conduct DDoS attacks; once the extortion payments were made, executors were paid and parted ways with their employers. The life-spans of cybercriminal organizations were eminently transient in nature.

In chapter two, I suggested that criminal techniques required the convergence of different ICTs, resulting in networked attacks. Indeed, DDoS attacks were networked with botnet herders using Trojans to remotely infect computers and then link them in many combinations to create botnet assemblages. Other techniques were also networked, with each component responsible for a specific task, as demonstrated by the use of rootkits. Here, each malware in Gambling Federation's software conducted a deterritorialization movement; one Trojan was responsible for relaying customers' keystrokes back to hackers, while another interfered with nodal connectivity denying customers access to other gambling sites. Indeed, these attack assemblages permitted a complex interplay of numerous techniques, making crime diverse, adjustable, and easier to commit in cyberspace than in physical space. Cybercriminals incorporated several mediums in their interactions, resulting in an intricate communication assemblage. For example, several cybercriminals used emails, hacking communities, and underground servers to communicate as was evident with the identity theft ring that targeted BetOnSports.com. Here, Elekede employed two email accounts to communicate with his associates, while using underground servers to interact with customers who bought the stolen company database. As my integrated theory stated, cybercriminal organization was

also an assemblage with no set hierarchy and ephemeral partnerships, as demonstrated by the colluding alliances between Vaughn and Mizzi at FullTiltPoker.com, Potripper, #363, GrayCat, PayUp, and SteamRoller at AbsolutePoker.com, and the disgruntled customers and insiders at BetOnSports.com. In each case, members were not committed to set partnerships and were relatively disorganized in structure. Even though these associations lacked stability, they practiced an egalitarian division of labour. For instance, Vaughn was responsible for playing most of the poker tournament at FullTiltPoker.com, while Mizzi took over during the final game. Similarly, #363 had insider access to everyone's cards, and was responsible for relaying this information back to his accomplice, Potripper, who had the task of defeating honest players using this information. At BetOnSports.com either disgruntled customers paid company employees to obtain insider access to the company's accounts and passwords, or employees gave the customers access to company servers, in order to deface BetOnSports' site for dissatisfactory customer and employee services. The underground botnet economy also had a loose networked structure with a division of responsibility amongst malware authors and bot-herders; writing and disseminating malware, as well as remotely controlling botnet armies, were equally important to maintaining the botnet economy. Finally, sub-networks within cyberextortion rings distributed their tasks; organizers planned and coordinated criminal activities, extenders recruited the appropriate executors to expand the criminal organization and acquire the necessary skill-sets, and the executors implemented DDoS attacks against gambling sites. Thus, each member had equal importance; no member was in charge of the entire criminal operation, and this resulted in a lateral assemblage with minimal striation.

Criminal techniques were conducted along an assortment of flight lines, as illustrated by the various digital trajectories of techno-nomads. For instance, JJProdigy connected directly via a single flight line to PartyPoker.com, where he used multiple accounts to cheat. Other cheaters used the PokerSmoke bot to connect to online poker rooms indirectly; they first connected to the bot, which then linked to the poker site (double flight line). These trajectories were still different from those used by digital associates. For example, Vaughn and Mizzi's cheated at FullTiltPoker.com by logging in through different computers, using different trajectories to engage in the deterritorialization movement of online seat-stealing. Thus, multiple trajectories were used by techno-nomads and digital associates to cheat at gambling sites, which made the cheating/collusion activity adaptable and easier to accomplish. Cyberextortion rings also used numerous trajectories; first several paths were used to install Trojans on computer systems worldwide, then the bot-herder used multiple paths to remotely control these machines, and finally, these paths attacked the targeted gambling site via numerous flight lines. Thus, not only were the flight lines different for techno-nomads, digital associates, and striated assemblages, but trajectories were also different *within* each type of criminal organization depending on the type of crime being committed; as noted above, the flight lines of different techno-nomads (JJProdigy vs. PokerSmoke bot-users) varied as they engaged in different deterritorialization movements (multiple accounts vs. AI software). Cybercriminals communicated with each other via multiple flight lines. Techno-nomads and digital associates worldwide, for example, connected to an assortment of newsgroups, IRC channels, and hacking websites to exchange information, offer advice, obtain the latest criminal techniques, and form alliances. Cybercriminal organization also

formed and operated via multiple flight lines. As techno-nomads operated alone, they did not require any paths for criminal organization. The digital associates who engaged in seat-stealing, met online to exchange ideas, form alliances and coordinate collusion activities, demonstrating the use of several networking flight lines. The cheaters then used separate flight lines to conduct their tasks based on the division of labour; Vaughn played most of the game, and then Mizzi relieved him during the FullTiltPoker.com tournament finale. The trajectories of striated assemblages involved different sets of flight lines for each sub-group of the assemblage. For instance, in a cyberextortion ring, the extenders' trajectories involved accessing the numerous hacker bulletin boards and underground economies to recruit hackers; the trajectory of executors not only involved accessing these sites to create contracts with cyberextortion rings, but also involved accessing hacking communities to find information and recruit associates to commit DDoS attacks. Thus in line with my integrated theory, cyberspace harboured diverse nomadic movement along a multitude of flight lines, making cybercriminal techniques and organizations dynamic, opportune, flexible, and transient.

Finally, I argued in chapter two that cybercrime techniques were inherently structured to manage threats of reterritorialization. Clearly, some techniques handled reterritorialization threats by using revised deterritorialization movements, as was evident with the SoBig virus that was continuously revamped and released into the digital wilderness. This trait was also exhibited by the PokerSmoke bot and the Holdem' Genius software that were appraised and upgraded regularly so as to enhance their quality and scope for criminal events. Other techniques used regeneration. Bot-net armies were often disposable entities; hackers easily compromised machines and redeployed new ones with

ease and efficiency. Similarly, the MaxLotto site also exhibited regenerative qualities by appearing, disappearing, and reappearing in cyberspace. Finally, criminal activity sometimes vanished entirely. Botnets, for instance, were designed to self-destruct when someone other than the original herder attempted to control them. Cybercriminal communication channels changed frequently; to avoid creating set patterns, multiple email accounts were used by members of the identity theft ring that targeted BetOnSports.com, and carders used different underground servers, such as Shadowcrew.com, CardersMarket.com, and CarderPlanet.com, to network with, and sell digital loot to, other cybercriminals. Different types of criminal organization managed reterritorialization threats in two ways. Techno-nomads and digital associates simply disappeared along multiple flight lines in smooth space. The hacker who executed DDoS attacks against gambling sites in the Shadowserver case vanished after conducting a few 'test-runs'. Likewise the digital associates operating MaxLotto.com disappeared along different flight lines; the current location of several associates in the MaxLotto scam was unknown. Components of striated assemblages also disappeared into cyberspace. The SoBig virus writers disappeared along different flight lines upon learning that several security and law enforcement agents were actively looking for them. Striated assemblages also used regeneration tactics; the void created in the Euromillion Espana lottery fraud upon the apprehension of several scammers, was immediately filled by new scam artists. Thus, cybercriminals and their digital techniques managed reterritorialization threats using disappearance, modification, and regeneration, which supported several claims in my integrated theoretical framework.

In sum, my theoretical framework was supported by the data collected in preceding chapters. My perspective accounted for how cyberspace and ICTs altered criminal organization, operation, and communication along the six dimensions of space, scope, time, movement, structure, and preservation. The case data, however, also raised several questions about the *scope* of my integrated framework, and implied that some elements of cybercriminal organizations and operations did not occur exclusively in cyberspace.

Theory Questioned

While my integrated theory adequately accounted for criminal organization and operation that occurred *solely* in digital environments, some components of crimes at gambling sites operated in *physical* space and did not fit well with my theoretical framework. My data indicated that some cybercriminals still used traditional criminal techniques. For instance, the identity theft ring that targeted BetOnSports.com kept details of victims' confidential personal and financial information as well as the contact information for other criminals in notebooks and not in computers, indicating that traditional modes of recordkeeping still existed for online crime. Also, the online Euromillion Espana scam included the use of classic Nigerian scam techniques. Social engineering methods used emails, as well as personalized phone calls, fake PO boxes, addresses, and forged company documents, which made the scam seem trustworthy. More substantively, members of digital associations and striated assemblages met and organized in both physical and digital space. For example, alliances for the online lottery scam in India were created at Acharya's shop, where Albaika and Acharya met face-to-face, and Sagwekar met Acharya in person to hand over cash withdrawals. The digital

associates who co-founded MaxLotto had met each other while working at Lehman Brothers and operated the fraudulent site for two years, demonstrating that these associates knew each other in real space and cooperated for a longer time frame than evinced in the cyberspace operation. Furthermore, online alliances were not entirely anonymous or fleeting, as my theory had suggested. The FullTiltPoker case revealed that Vaughn and Mizzi met online and were 'friends'; it was unclear whether they knew each other's real identities, but they had interacted on several previous occasions and were known to each other in cyberspace. The Giordano case also demonstrated the importance of face-to-face member contact and long-lasting alliances; Giordano, his wife, daughter, and son-in-law had important roles in the criminal operation, indicating that kinship ties still existed in some online criminal operations. Familial and friendship ties were also evident in the Uvari bookmaking group, where Uvari, his bother, and son, and their friends Meyerowitz and Appelbaum, collectively operated the criminal network. Thus, unlike the anonymous and fleeting alliances created in cyberspace, these members, like Best and Luckenbill's (1982) peers and mobs, knew the identities of their partners and worked together with little turnover in membership. The sustenance of these offline ties and alliances were not accounted for by my theory, which assumed that all criminal organization involved weak bonds, fleeting relationships, and anonymity.

My data suggested that some cybercriminal organization occurred in physical space, along with varying degrees of online presences. For instance, Albaika was the only associate in the Indian lottery scam who operated in cyberspace by sending emails to potential victims; Acharya and Sagwekar operated entirely in the physical terrain to move the money. Similarly, the only online associate in the MaxLotto fraud was the 'Cable &

Wireless' company who managed the fraudulent site; the co-founders and the marketing subsidiary organized themselves in physical space. Some striated assemblages such as the Giordano money laundering group and the Starnet fraudsters had sub-networks that were located predominantly in physical space with only a few online sub-networks. The Giordano organizers, controllers, financial officers, clerks, agents/runners, distributors, and accountants, operated in physical space, while its executors (Primary Development and Digital Solutions) operated in cyberspace. Similarly, the Starnet scam involved CEOs and accountants who planned the fraud and laundered illegal proceeds in physical space, while only the site operators functioned online by tampering customer records, modifying betting histories, and generating fake winners. Other striated assemblages, had equal presences in digital and physical environments. For example, the organizers of several cyberextortion rings, such as the Russian, Middle Eastern, and Asian organized crime groups, operated in physical terrains. Extenders and executors worked primarily in the digital terrain, with the former recruiting the latter to carry out DDoS attacks. The money mules, on the other hand, picked up extortion payments in physical space, while money movers wired illicit funds through untraceable networks in cyberspace. These case studies clearly illustrated the importance of physical space in the organization of cybercriminal groups, something that was downplayed in the early formulation of my integrated theory.

Furthermore, while cybercriminals were able to evade reterritorialization threats through disappearance and regeneration along multiple flight lines in cyberspace, this did not always protect cybercriminals, who were sometimes exposed in both online and physical spaces. For example, PartyPoker.com operators discovered JJProdigy's cheating

activities in cyberspace; like Best and Luckenbill's (1982) 'loner', he was susceptible to detection, and the multiple flight lines for escape did not guarantee his safety. The FullTiltPoker.com operators detected Vaughn and Mizzi using the same user account from different IP addresses, demonstrating that digital associates were also exposed in cyberspace. Indeed, some digital associates were detected in physical space; the money operators in the Indian lottery scam were apprehended in physical space, and they then revealed the identity of their online associate. Many striated assemblages were exposed in cyberspace, such as the Russian cyberextortion ring, whose activities were traced and monitored online. But other striated assemblages, such as the Giordano group, were exposed in both digital and physical spaces. Police tracked Giordano's activities and phone calls in physical space, while online money laundering activities were monitored in cyberspace after Giordano's computer was cloned. These findings indicated that my assumption that cyberspace effectively protected cybercriminals and their operations from detection required rethinking; regardless of the sophistication of the criminal organization, techno-nomads, digital associates, and striated assemblages were sometimes vulnerable to exposure in both cyberspace and physical space.

Clearly my integrated theory was unable to account for some aspects of criminal organization at gambling sites; it did not explain the full nature of alliances, account for the interaction of criminals in both physical space and cyberspace, and allow for the possibilities for detection. In the next section, I address these shortcomings, reformulate three concepts in my integrated theoretical framework and demonstrate how these reforms improve its applicability.

Theory Revisited

While a majority of my findings support my integrated theory with respect to criminal organization *shifting* to cyberspace, the preceding discussion indicates the need to refine the concepts of space, time, and criminal structure to account for this interaction between physical and digital spaces in criminal events.

Hybrid Spaces and Criminal Movement

To start we need to conceptualize a new space for crimes in *hybrid* space. In hybrid space, cyberspace is contiguous to physical space; both spaces are mutually constituted and neither physical nor digital space is predominant. Here, individuals move to commit crimes by 'jacking into' cyberspace and 'disconnecting' to return to physical space. This ability to move between two environments in hybrid space creates hybrid criminals, or what I call *hybriminals*. In hybrid space, notions of space, site, and distance are different from those conceptualized solely in cyberspace. Hybrid space is both finite and infinite, sites are both remote and proximate, and distance both exists and disappears. For example, hybriminals can jack into cyberspace to experience an infinite space, where they can attack a targeted site directly or remotely through an endless combination of flight lines. Here, distance is a malleable entity. But hybriminals can also 'disconnect' to return to physical zones where distance is fixed and space is finite. Thus, hybrid space *extends* cyberspace; cyberspace may be infinite in its scope, but hybrid space is both infinite and finite. This duality of space and site (finite/infinite, remote/proximate) increases the scope of hybriminal movement and organization. While sites of victimization may be in cyberspace, sites of perpetration, interaction, coordination, and network formation may exist in both the physical and digital terrains of hybrid space.

Hybriminals can meet in physical zones in close proximity and then jack into cyberspace to remotely attack sites worldwide. Alternatively, hybriminals can commit crimes online, and fearing exposure can disconnect to escape into physical zones. This ability to fluctuate between space, site, and distance gives hybriminals even greater control over their movement and organization than I had surmised in chapter two; they can control their points of arrival and departure, direction, and the distance traversed in hybrid space.

Temporal Simulacrums and Criminality

As we have seen, some components of criminal organizations in hybrid space are located *simultaneously* in digital and physical spaces. The life-span of the hybriminal assemblage is thus determined by the duration of both its physical and digital sub-components, resulting in long-term and short-term life-cycles. For instance, the physical sub-component may exist over an extended time frame, while online components formulate, dissolve, and regroup intermittently. Additionally, hybriminal movement in digital zones is fast, pliable, and dynamic, while movement in physical zones is slow, fixed, and preset. Thus, hybriminals can calibrate the speed of their movement; they can 'fast-forward' by jacking into digital space or experience 'slow-motion' by traversing physical space. Hybrid space allows cybercrimes to be committed synchronously/ asynchronously, continuously/intermittently, concurrently/chronologically, in real/chosen time, and for short/long time periods. Bogard's (1996) work on the simulation of surveillance is useful for conceptualizing cybercrimes as a series of *breaks* and *flows*; cybercriminals can completely control cybercrimes to "enhance them, speed them up, slow them down, repeat them, knock them off course, [and] cancel them" (p. 43). Furthermore, criminal techniques are often turned into *copies*; for example, Trojans and

hacking toolkits are reproduced endlessly and recirculated continuously through cyberspace (Bogard 1996, p. 45). These copies are *better* than the original; they are constantly updated as they are replicated to fix defects and improve quality. Thus, cybercrimes occur in temporal simulacrums; cybercriminals become ultimate time keepers as they have almost absolute control over their criminal activities, or so they imagine.

Hybrid Assemblages and Hybrid Crimes

My integrated theory suggests that organizations operating solely in cyberspace are lateral, with a weakly developed horizontal division of responsibility, and often fleeting memberships. Hybrid organizations, however, exhibit the characteristics of both land-based and digital criminal organizations. For instance, hybriminals find confederates in both physical and digital spaces, depending on which skill-sets they require; technological skills can be found in digital environments, while traditional skills are discovered in physical space. Thus, the hybriminal organization has access to a larger set of criminal expertise, which determines unique possibilities for alliances and divisions of labour. Furthermore, these hybrid organizations can have both weak and strong ties simultaneously. For example, an organized crime group can have long-term membership based on kinship and strong familial ties, while hiring cybercriminals on a contractual basis. While a majority of cybercrimes are conducted entirely in cyberspace, some crimes require physical components. These crimes may operate as an assemblage of old and new attack techniques; hybriminals not only interconnect different digital techniques, such as emails, viruses, and phantom sites, which exhibit networked characteristics in and of themselves, but they also deploy traditional techniques, such as social engineering,

forgery, cash pick-ups, and money laundering. These criminal techniques function together as an assemblage to complete cybercrimes. Thus these three revised concepts of space, time, and criminal structure, modify my integrated theory so as to address the limitations identified earlier. So what are the theoretical effects of these conceptual revisions?

Theory Evaluated

Theories range greatly in their degrees of formal development. Since my research was exploratory, it did not employ a formalized theoretical framework for analysis because such a framework was absent in the criminological literature. So, I endeavored to generate six properties of cybercrime and cybercriminality by drawing from theories on criminal organization and cyberspace. I developed the six concepts of space, time, scope, structure, movement, and preservation, to analyze cybercrimes at gambling sites and modified them to address several empirical limitations. This impacted the scope, coherence, explanatory capacity, and predictive power of my integrated framework.

Scope

Wagner (1984) and Shoemaker, Tankard, and Lasorsa (2004) state that theories should be evaluated on the basis of scope, by which they mean the comprehensiveness of the account of a particular problem. Theory growth, they say, may occur in two ways. First, the designed theory may be compared with its alternatives. I use Brenner's (2002) and Wall's (2007) work on cybercrime as a departure point to create an integrated theory in chapter two. Brenner (2002) focuses exclusively on organized cybercrime; individual and small-scale partnerships, however, are not addressed in her work. Wall (2007) discusses the impact of cyberspace on the organization of crime, criminals, and their

communication, but he does not offer a comprehensive set of theoretical concepts to analyze their organizational dynamics. My integrated theory develops Brenner's (2002) and Wall's (2007) ideas to form a more elaborate theoretical grid; it proposes the six dimensions of space, scope, time, movement, structure, and preservation, and uses these concepts to account for both the descriptive and theoretical understanding of the organization of cybercrime, cybercriminals, and criminal communication. Second, theoretical growth may be evaluated by comparing theory with observations. While my research does not conduct a scientific study resulting in empirical observations, it uses case studies as data substitutes to assess the relevance of theory. The concepts of space, time, and structure are refined to address previous limitations, which further expands the scope of my integrated theory. Indeed, my revised theoretical framework goes beyond accounting for the organization of criminals, crimes, and communication in cyberspace; it now conceptualizes these three elements in what I call hybrid space. Thus, a more probable and comprehensive picture of the nature of alliances, their durations, the marriage of digital and non-technical criminal expertise, the evasion and neutralization of crime prevention tactics, and the organizational vulnerabilities, is attained using the revised integrated theoretical framework.

Coherence

A theory is internally coherent if its concepts rationally interconnect with, and do not contradict, each other; concepts should be "logically related, build on each other, or contribute to the explanatory power of each other" (Swenson 1999, p. 2). While my theory was still in its infancy and had no formalized propositions, the concepts put forth by my theory did not contradict each other; they complemented each other to suggest a

reasonable picture of online crime and criminality. In chapter two, my integrated theory proposed the concepts of space, scope, time, structure, movement, and preservation. The organizational dynamics of cybercrimes and cybercriminals could not be explained by a single concept; these concepts were logically related as each could not be explained without the other while accounting for the organization of crime and criminality in cyberspace. The need to modify my integrated theory, however, did not mean that my theory was internally incoherent. By refining the concepts of space, time, and structure, the other concepts of scope, movement, and preservation were indirectly refined, clearly indicating that these concepts built on each other. Furthermore, the revised concepts were still logically related; the concepts of hybrid space, hybrid time, hybrid structure, scope, movement, and preservation still overlapped to explain the organization of online crime and criminality. For instance, movement was explained in relation to hybrid space and hybrid time, and preservation in terms of hybrid space, hybrid time, movement, and structure. Indeed, my proposed concepts were rationally connected and contributed to each other's explanatory capacity.

Causality

As Einstadter and Henry (1995) note, the "purpose of all theory is to understand and explain" (p. 12). While my integrated theory is not fully developed to offer a complete explanation for how criminals organize themselves and their crimes, my research attempts to identify the factors that shape these organizational properties. My theory adopts an interactive causality model of causal explanation, where causal factors (the six concepts/variables of space, scope, time, movement, structure, and preservation) influence each other, such that crime and criminality are an outcome of this interactive

process (Einstadter & Henry 1995, p. 15). For instance, space, time, and movement, determine the organization of criminality (criminals meeting in cyberspace to form alliances in real-time); here the variables determine the organization of cybercriminals. Furthermore, the variables can impact each other; for instance, movement and preservation determine time (cybercriminals move along flight lines to escape policing threats, resulting in a criminal organization with a short life-span). The revised concepts still influence each other; hybrid space, for instance, determines the scope and movement of cybercriminals and their crimes. Indeed, my modified integrated theory still follows the interactive causality model. The interaction of these revised variables plausibly determines the organization dynamics of criminality and crime; for instance, hybrid space, hybrid time, and movement determine the organization of hybriminality (criminals could organize in both physical and digital space in real/chosen time, and have short-term or long-term alliances).

Predictive Power

Shoemaker, Tankard, and Lasorsa (2004) state that one way to evaluate theory growth is its ability to make predictions; the "more precise the prediction, the better the theory" (p. 173). My integrated theory is still in formation and does not yet include a formalized set of propositions that can accurately predict the organization of cybercrimes and cybercriminals in *all* contexts. Nevertheless, a majority of general assumptions about the organizational dynamics of online crime and criminality put forth by my integrated theory in chapter two, resonates in the data, suggesting that these assumptions reasonably account for the formation of cybercrime and cybercriminals. While the earlier version of my theory was unable to account for hybrid space, the reformation of space, time, and

structure improves my theory's ability to plausibly predict which components of cybercrimes occur in physical and digital environments. Furthermore, my revised integrated theory is inductive; by examining the specific phenomenon of cybercrimes at gambling sites, my theory is assessed and revised to make generalizations of the organization of hybriminals and hybercrimes.

My revised integrated theory allows me to generate a preliminary proposition or an equation for future research; the organization of cybercrime and cybercriminality (OC) can be expressed as a function of the six dimensions of hybrid space (HS), hybrid time (HT), hybrid assemblage (HA), movement (M), scope (S), and preservation (P). Thus:

$$OC \approx f(HS, HT, HA, M, S, P)$$

In conclusion, the modifications to my integrated theory improve its scope, coherence, causality, and predictive capacity, as well as offers a generalized proposition, which ultimately results in theoretical growth. As this proposition is tested in new and/or alternate settings, my theoretical concepts will be reformulated; indeed my integrated theory will move to a "closer approximation to the truth" as time passes, by reshaping and refining itself (Shoemaker, Tankard & Lasorsa 2004, p. 174; Skidmore 1975, p. 16)

Conclusion and Future Research

My thesis has explored the area of cybercrimes at gambling sites; I have illustrated the complexity of this phenomenon by revealing the typologies of crimes and the assortment of digitized techniques used by cybercriminals. Furthermore, situating my research in the online gambling context has allowed me to uncover the various ways in which criminals organize in hybrid space, an area which has remained unexplored in the fields of criminology and gambling studies. My data has clearly indicated that

cybercrimes and cybercriminals had various components of their organization in both physical and digital terrains, challenging my earlier assumption that they operated exclusively in cyberspace. By modifying my integrated theory to account for the relevance of hybrid space, I have offered a comprehensive set of concepts to understand the organizational dynamics of crime and criminality. My study has served as a preliminary attempt at constructing a socially structured explanation of the organization of cybercrimes and cybercriminals. It has attempted to move beyond the simple definitions and typologies of conventional criminal organization approaches and has sought to comprehend the organizational dynamics of both crime and criminality in hybrid space as a problem definable by criminological theory. Furthermore, my research has offered a theoretical proposition that can help drive future research.

Indeed, one area of research can test this proposition by conducting an ethnographic study of cybercriminals. While my research employs case studies based on secondary sources, future research should permit cybercriminals to speak for themselves; accessing the sources directly will reveal their characteristics, rationales, motivations, and organizational dynamics that are more thorough and complete than is the case in my study. Future researchers might interview apprehended cybercriminals face-to-face in prison settings to address several issues: (i) justifications for operating alone or with confederates, (ii) duration of alliances, (iii) division of labour, and (iv) factors leading to their detection and apprehension. Researchers might also conduct virtual ethnographies by accessing networking sites, such as hacking forums, newsgroups, and bulletin-boards to obtain textual transcripts of cybercriminal conversations. Combining these two research methods takes into account both physical and digital venues of criminal

organization. Researchers can then compare the organizational differences between apprehended and undetected cybercriminals, which I think would shed light on the characteristics of successful cybercriminal organization. Furthermore, this research can determine the adequacy of my proposition by analyzing the importance of all six dimensions of space, time, movement, structure, scope, and preservation, as well as which ones are more relevant in determining cybercriminal organization. Thus, this research can improve the *scope* of my integrated theory.

The *range* of my theoretical framework can also be improved by assessing its applicability to other cybercrimes, such as software piracy. Researchers can examine case studies of software piracy in other institutional contexts to identify apprehended criminals and illegal software dissemination sites used by cybercriminals. Researchers can then use this information to interview the arrested criminals in prison settings to determine the techniques they used to illegally obtain, copy, and distribute pirated software, and the communication avenues they used to engage in this illegal enterprise. Researchers may also interview law enforcement agents who conducted 'sting' operations to study their techniques, such as monitoring and infiltrating software piracy rings, and the employment of "honeypots" (trap websites to lure cybercriminals). Finally, software companies, such as Microsoft and Corel, can be interviewed to examine specific industrial measures used to prevent software piracy. Together, these methods allow researchers to study three objectives: the organizational dynamics of software piracy rings; the techniques for operating such rings (illegal procurement of software, its replication, and dissemination); and the adequacy of digital countermeasures employed by law enforcement, private security firms, and software companies.

My study explores the different types of cybercrimes at gambling sites; a third area of research might conduct in-depth studies into a particular type of cybercrime, such as cheating. Here, research could focus on an assortment of gambling sites, such as blackjack, poker, bingo, craps, and roulette to identify cheaters and their specific cheating techniques. Researchers might include a comparative study of different corporate websites. A three-step methodology might be utilized. Researchers could first obtain case studies to identify media accounts of cheating in order to identify apprehended cheaters. Researchers could then interview the cheaters to learn about techniques used, colluding associates, and reasons for their exposure and arrest. Finally, researchers could observe each gambling site to identify cheating activities in progress in order to examine specialized techniques and collusion properties. Combining these methods could permit researchers to delve into the area of cheating. This research might address three objectives. First, it could offer an in-depth typology of cheating techniques, such as manipulating software and random number generators (RNGs), and using bots and insider information. Second, it might propose a detailed typology of cheaters, such as individuals, partners, unscrupulous site operators, and the characteristics of cheating, such as information exchange, channels of communication, and types of agreements. Third, it could analyze the links between the two typologies to identify which techniques are used by cheaters at different gambling sites. Overall, this study would offer a criminological perspective on the understudied area of cheating at gambling sites, rather than the technical studies that are currently found in the field.

Finally, my research suggests that gambling sites commit fraud against their customers and licensees. This finding can trigger a fourth research area: the prevalence of corporate crime in the online gambling industry. Research can examine the case studies (BetOnSports, MaxLotto) presented in my research along with other data to identify the perpetrators of corporate crimes (CEOs, site operators), the types of crimes (cheating licensees, withholding payouts), and the techniques of apprehension (security and law enforcement measures). Researchers can use this information to conduct interviews with (i) corporate criminals to determine their culture and neutralization techniques to rationalize their criminal acts, (ii) whistleblowers to determine the inner-operations of corporate crimes, (iii) victims of corporate crime to identify how they were defrauded and what actions they undertook, and (iv) private and government security experts, law enforcement agents, regulatory bodies, and legal counsel to understand the actions taken to detect, apprehend, and punish corporate offenders. This research can address three objectives: examine the culture of corporate crime in the online gambling industry; investigate the techniques and organization of online corporate criminals; and study the global responses to online corporate crime, which surpasses geographical boundaries affecting victims worldwide.

This thesis employs a systematic methodology and case studies to study cybercrimes at gambling sites. It explores the organization of crime, criminality, and criminal communication in the gambling field, an area that remains underdeveloped in the criminological discipline. My study reveals that these three elements of cybercrimes do not occur exclusively in cyberspace; physical space still contributes to the organizational dynamics of cybercrimes and hybriminals. In light of this discovery, my

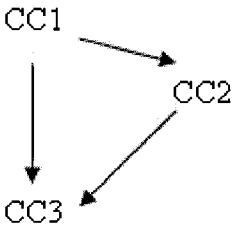
thesis develops an integrated framework that offers a reasonable conceptualization of crimes in hybrid space. In conclusion, this thesis serves as a point of departure for future studies; researchers can use some of the theoretical concepts I propose in this study to further assess, refine, and improve an integrated approach. Hopefully, this thesis will stimulate new ways of conceptualizing the organization, operation, and interaction of cybercriminals, ultimately contributing further to the fields of criminology and gambling studies.

Table 1. List of Keyword Combinations Used in Google

"internet gambling" + cybercrime	"online gambling" + cybercrime	bookmaking + cybercrime	"cyberextortion" + "internet gambling"
cyberextortion + "organized crime"	Cybercrime + "organized crime"	"online organized crime"	"online organized crime" + tactics + methods
cyberextortion + patterns + trends	cyberextortion + DDoS + botnets	hacking + "internet gambling"	hacking + techniques
hacking + tools	hacking + "identity theft"	hacking + software	hacking + motivation
"player collusion" + "internet gambling"	"cheating" + "internet gambling"	"cheating" + "online games"	"player collusion" + prevention
"player collusion" + security	"money laundering" + "internet gambling"	"money laundering" + "organized crime"	"money laundering" + "eCash"
fraud + "internet gambling"	fraud + "shell gambling sites"	fraud + "internet gambling" + winnings	fraud + "internet gambling" + payouts
"internet gambling" + underage	"internet gambling" + youth	"online gambling" + adolescent	"internet gambling" + youth + "identity theft"
cybercrime + combat	cybercrime + police	cybercrime + regulation	cybercrime + law
cybercrime + security	cybercrime + defense	Cybercrime + jurisdiction	cybercrime + prevention
cyberextortion + prolexic	cyberextortion + digidefense	DDoS + prolexic	DDoS + digidefense
"intellectual property theft" + cybercrime	"intellectual property theft" + software + "internet gambling"	"internet gambling" + netwar + rival	"internet gambling" + "digital war" + competition

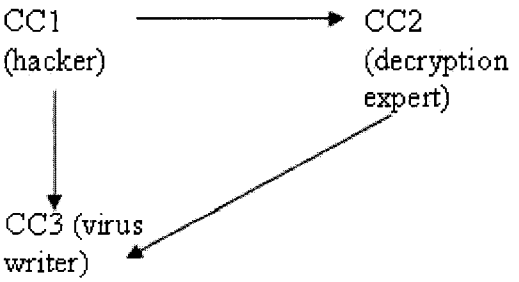
Figure 1. Rhizomatic Principles of Cyberspace

Connectivity



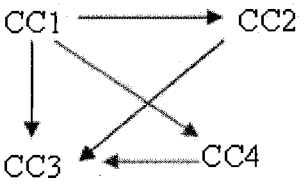
- No sequence or hierarchy
- Cybercriminals can connect with each other at any time
- Better flexibility

Heterogeneity



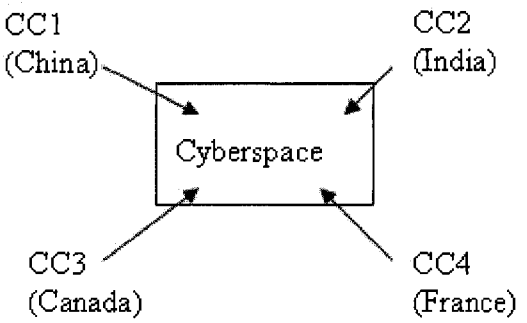
- Different skill sets useful for
  - Subculture
  - Division of labour
  - Better efficiency & flexibility

Multiplicity



- CC1 can link to CC3 in several ways spontaneously & sporadically => multiple linking opportunities
- Efficiency & flexibility

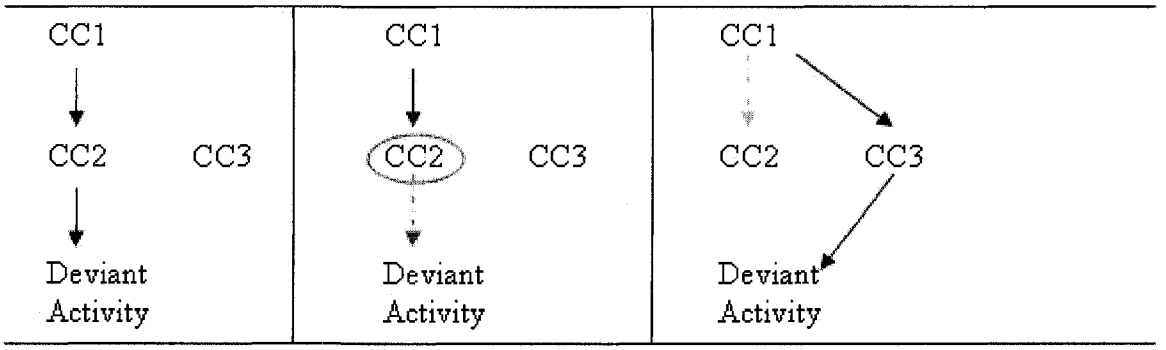
Cartography



- Cyberspace is a map – open & connectable; several entry points
- Subculture, learning & alliances

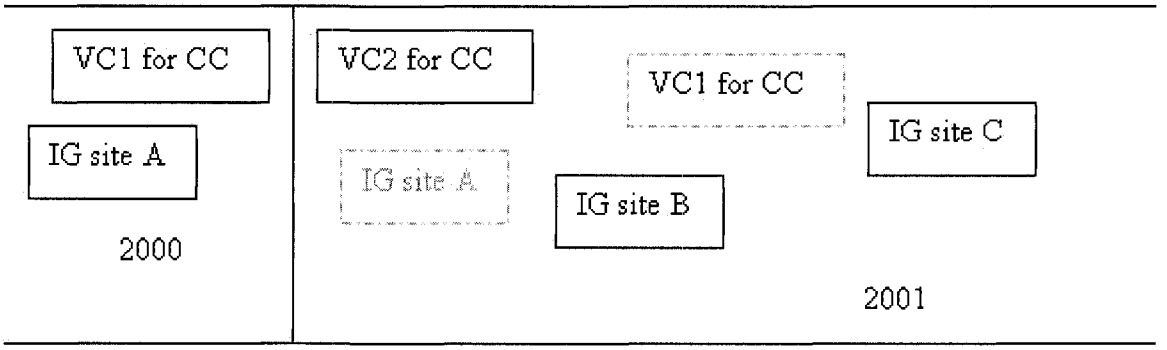
CC: CyberCriminal

Regeneration



- Detour around disruptions; broken link is creates elsewhere
- High turnover – fill (compromised) positions as required; temporary relationships between members
- Maintain operation
- Increased flexibility & adaptability -> survival

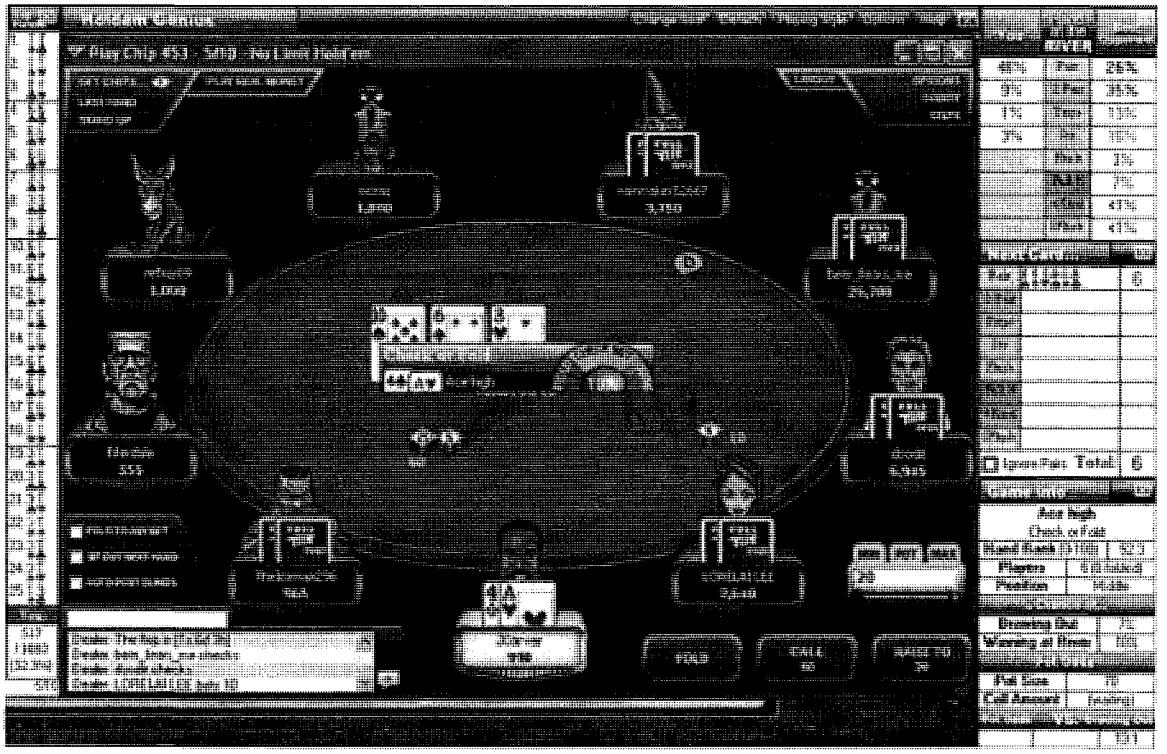
Decalcomania

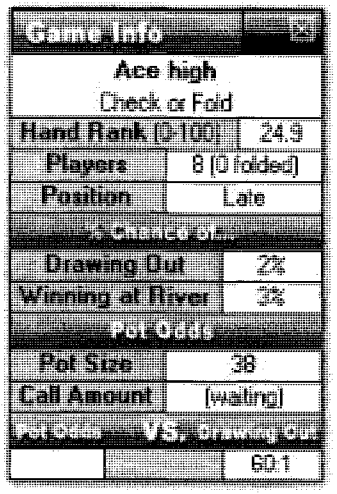


- Cyberspace has no structure; constantly changing; fluid, dynamic
- New targets constantly available
- New avenues of communication constantly available – avoid detection

VC: Virtual Community
IG: Internet Gambling

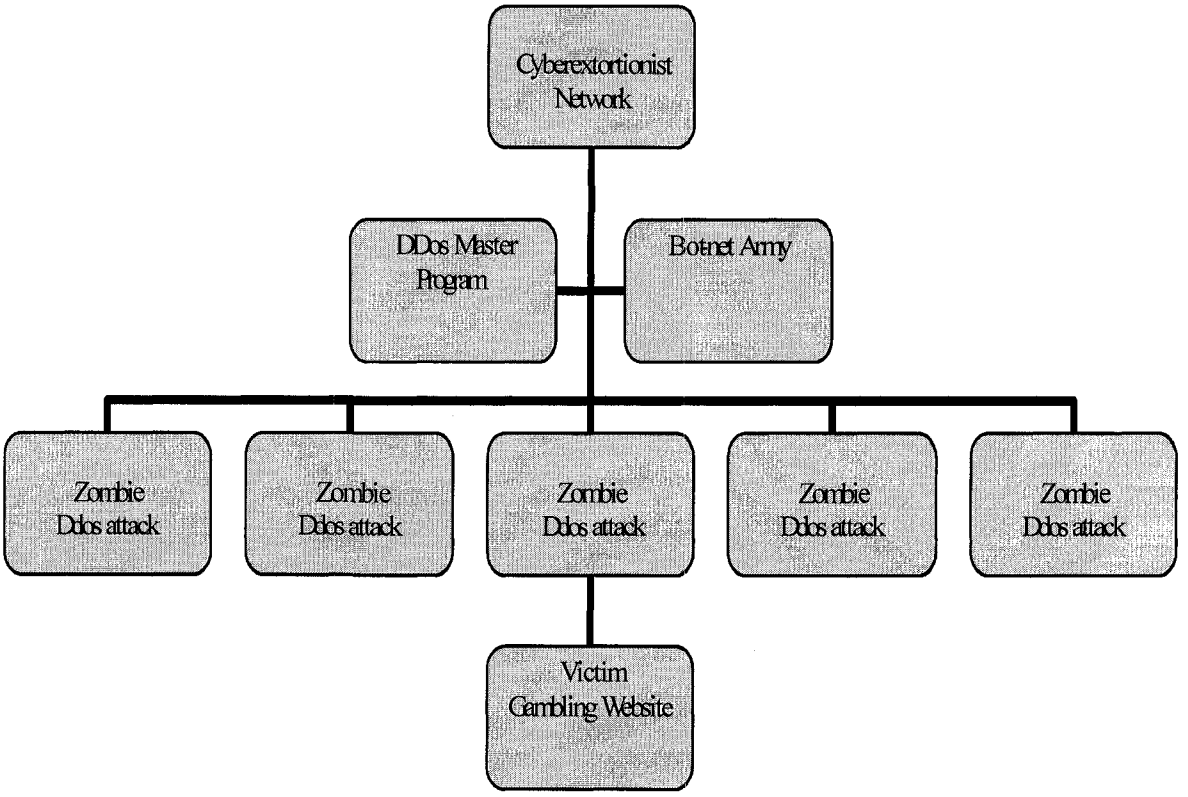
Figure 2. Holdem Genius Screenshots





Source: HoldemGenius (2008b). *Holdem Genius™ Screenshots*. Retrieved April 2, 2008. Online at http://www.holdemgenius.com/screenshots.html.

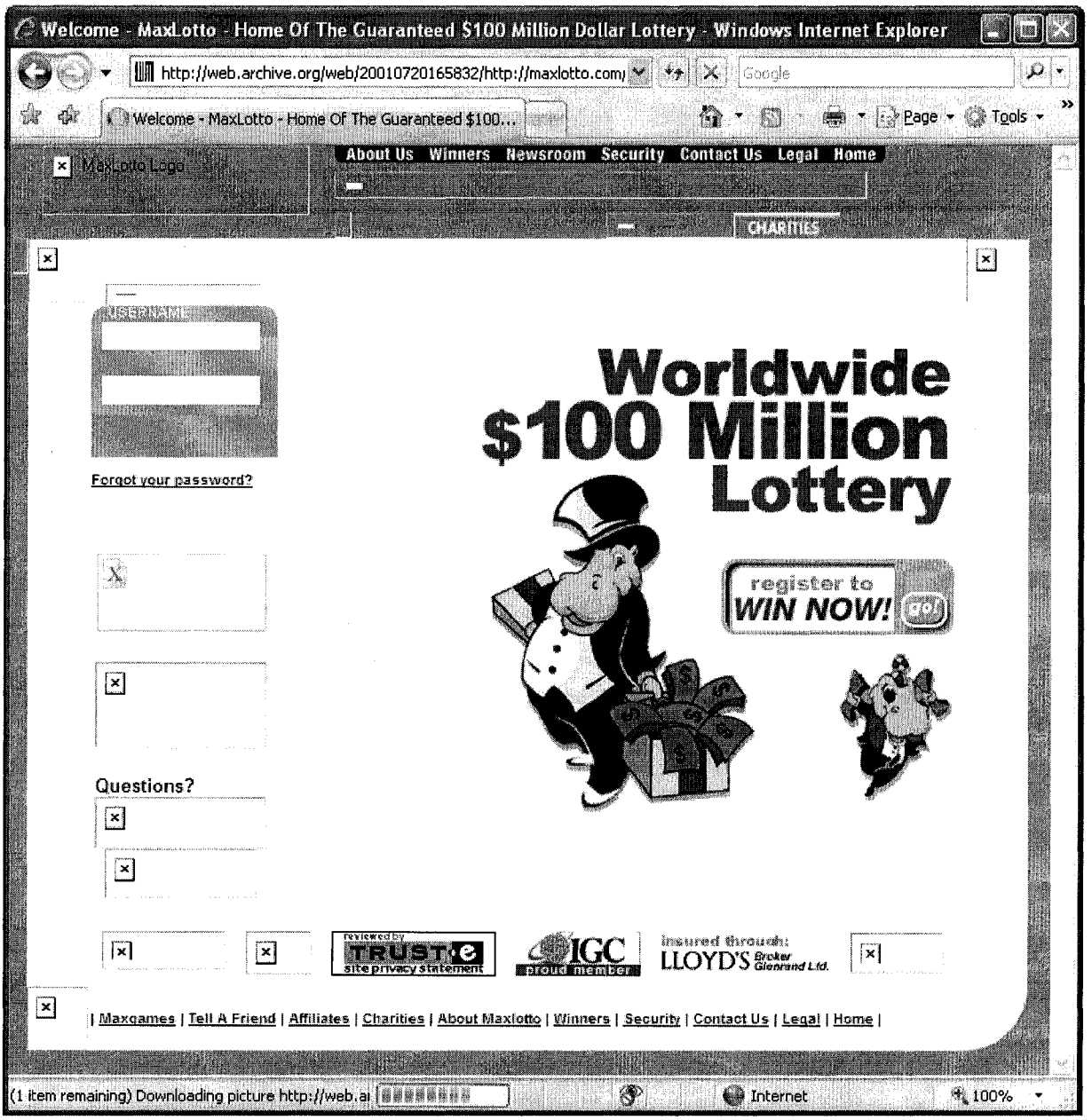
Figure 3. Diagram of a Typical DDoS Attack on Gambling Websites



Source: McMullan, J. & Rege, A. (2007). Cyberextortion at Online Gambling Sites: Criminal Organization and Legal Challenges. *Gaming Law Review, 11*(6), 648-665

Figure 4. Evolution of MaxLotto.com from 2001 – 2008

July 2001



Source: *web.archive.org*

May 2002


Welcome To MaxLotto - Home Of The World's Next Billionaire - Windows Internet Explorer
MAXLOTTO
Sorry, MaxLotto is currently upgrading.
We'll be back shortly.

November 2005

July 2006

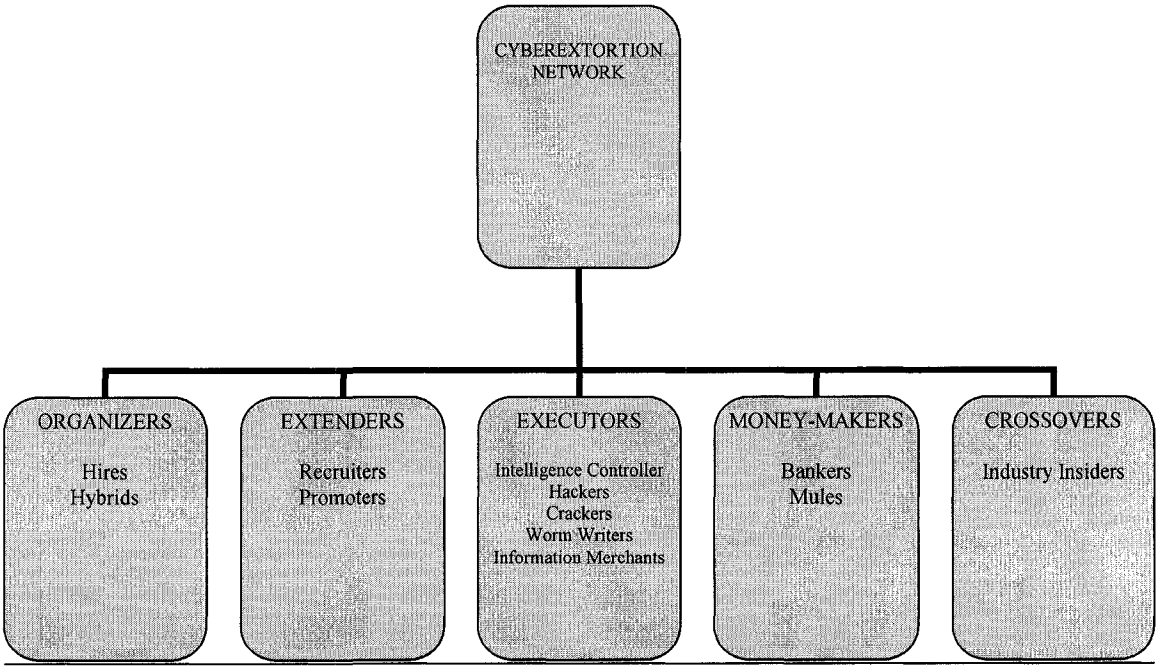

MaxLotto.com | Max Lotto - Windows Internet Explorer
http://web.archive.org/web/20060710020214/http://www.maxlotto.com/
Google
Internet Ex...
Maxlotto.com
MaxLotto.c...
MaxLot...
Page
Tools
MaxLotto.com
Related Topics
Online Casinos
Poker Online
Blackjack
Craps
Roulette
Sports Betting
Horse Racing
Las Vegas
Baccarat
Keno
Bingo
Slots
Casino Vacations
Most Popular Sites for LOTTERY
Casino-on-Net: Play Casino Games Online - Get 100% Deposit Bonus up to $200 FREE - Win REAL Money!
The Largest Online Casino offers cutting-edge games including: Blackjack, Roulette, Poker, Slots and much more. Up to $200 FREE Welcome Bonus. More than 20,000,000(!) Players Since 1997. Highest Payouts on the Net!
www.casinoonnet.com/
888.com: Voted Best Online Casino at 2005 Egaming Awards! $200 bonus & huge jackpots!
Download the BEST Casino Games for free and start Winning! 100% sign-up Bonus up to $200. The most trusted and reliable online casino since 1997 with the highest payouts on the net and more than 20,000,000 online players!
www.888.com/
$10,000 Daily Sweepstakes Entry
$10,000 given away every weekday!. Daily chances to win $ 1 million instantly! Plus, the grand prize - up to $25 million!
www.lynxtrack.com/
Internet
100%

January 2007

April 2008

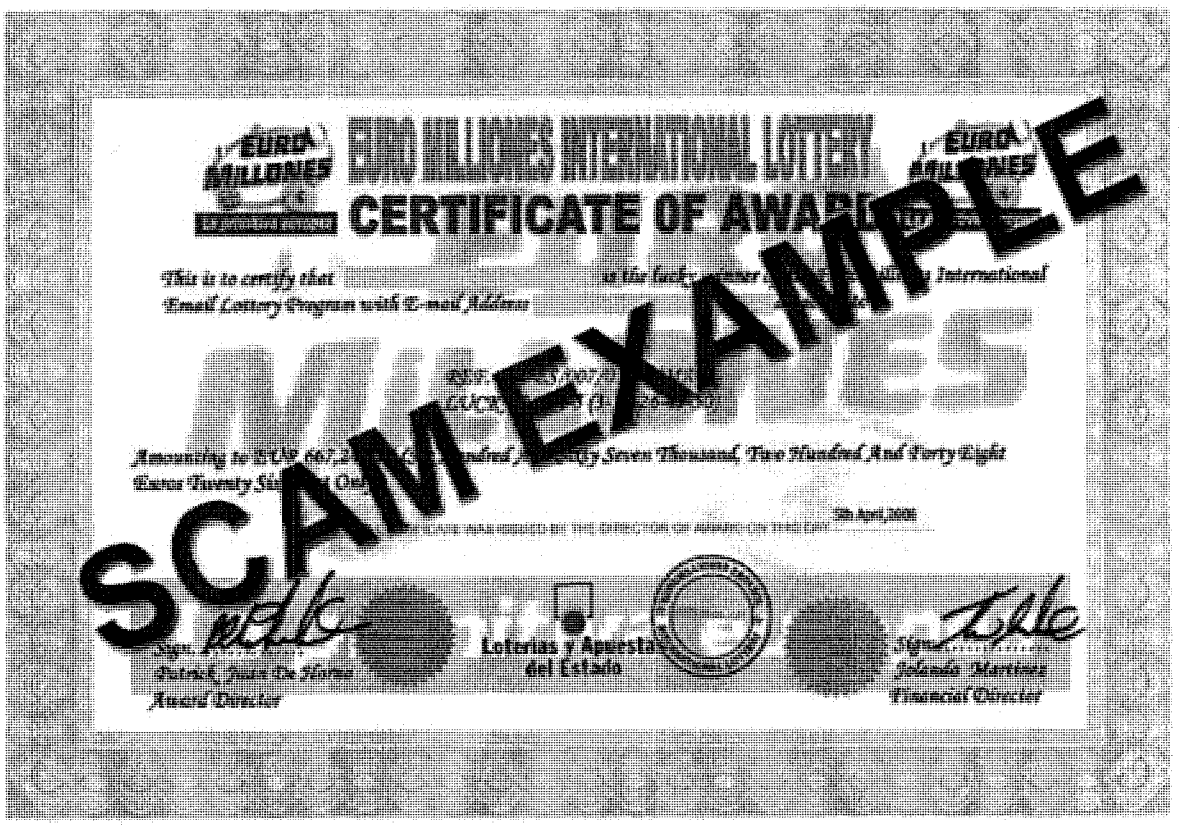

Maxlotto.com - Windows Internet Explorer
http://www.maxlotto.com/
Maxlotto.com
Page
Tools
Welcome to Maxlotto.com
Las Vegas
Las Vegas Casino
Las Vegas Hotel
Las Vegas Resort
Las Vegas Vacation
Las Vegas Reservation
Las Vegas Coupon
Las Vegas Deal
Las Vegas Discount
Las Vegas Entertainment
Las Vegas Concert
Looking for something else? Search for anything here:
Search
Check out our links for the most up to date Maxlotto information and much more!
LAS VEGAS | LAS VEGAS CASINO | LAS VEGAS HOTEL | LAS VEGAS RESORT | LAS VEGAS VACATION
Click to: + Bookmark this page.
©2008 Maxlotto.com
Disclaimer: Domain owner maintains no relationship with third party advertisers. Reference to any specific service or trademark is not controlled by domain owner and does not constitute or imply its association, endorsement or recommendation.
Internet
100%

Figure 5. Diagram of a Cyberextortion Network



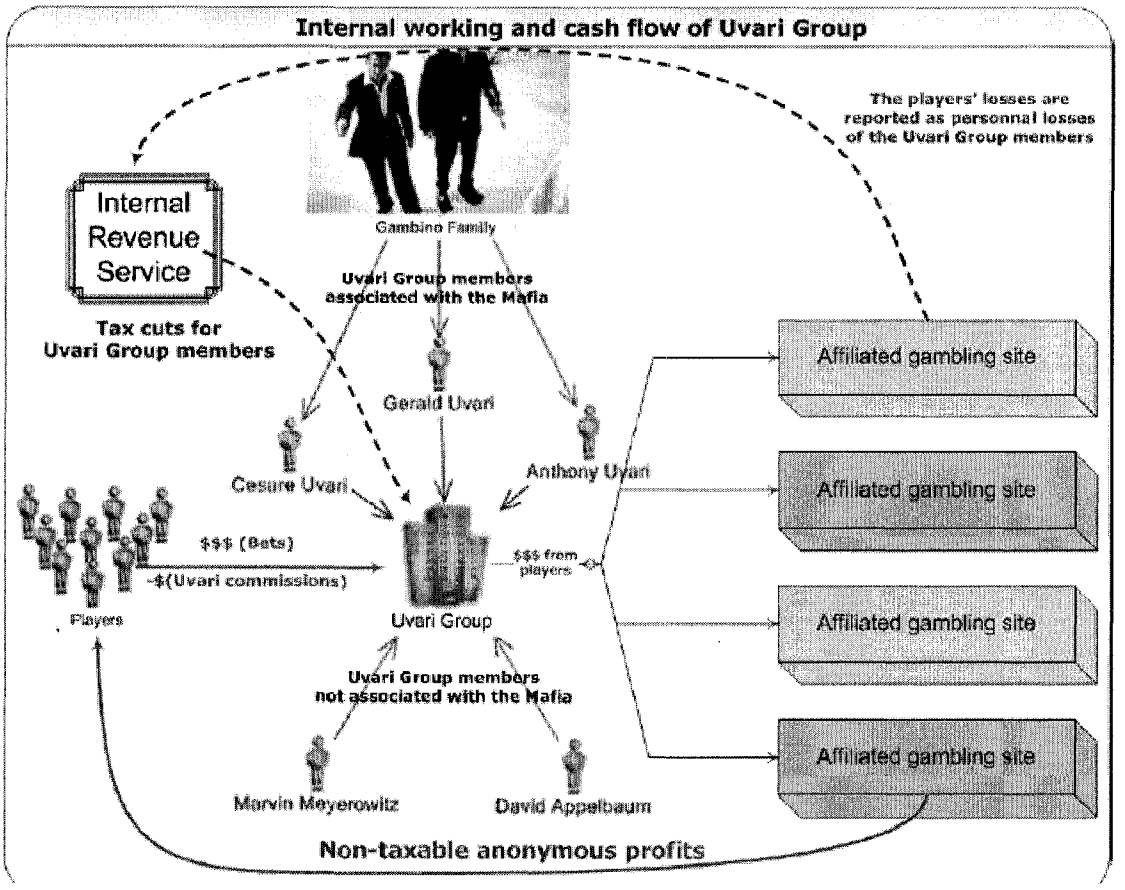
Source: McMullan, J. & Rege, A. (2007). Cyberextortion at Online Gambling Sites: Criminal Organization and Legal Challenges. *Gaming Law Review, 11*(6), 648-665

Figure 6. Euromillion Espana Scam Document



Source: Euromilliones.com (2006). *Attention Scam Letters & Emails*. Retrieved April 23, 2008. Online at http://www.euromillones.com/scams_euromillions.asp

Figure 7. The Uvari Group Bookmaking Scheme



Source: Computer Emergency Response Team - Laboratoire d'EXpertise en Sécurité Informatique (CERT-LEXSI) (2006). *Online Gaming Cybercrime: CERT-LEXSI'S White Paper*, July 2006.

References

Abadinsky, H. (1990). *Organized Crime*. Chicago: Nelson-Hall Inc.

Acohido, B., Swartz, J. & Ward, S. (2006). Cybercrime Flourishes in Online Hacker Forums. Retrieved November 14, 2006. Online at http://theadvertiser.gns.gannettonline.com/apps/pbcs.dll/article?AID=/20061012/TECH01/609070348/1001/tech

Adair, S. (2008). *Gambling Websites Under Attack*. Retrieved March 23, 2008. Online at http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080218

Albini, J.L. (1971). *The American Mafia: Genesis of a Legend*. New York: Appleton-Century-Crofts.

(AGCC) Aldernay Gambling Control Commission. (2006). *Internal Control System Guidelines. for eGambling*. Retrieved October 9, 2006. Online at http://www.gamblingcontrol.org/UserFiles/File/ICS20Guidelines202006.pdf

Ames, B. (2006). *Internet Gambling Operators Indicted*. Retrieved April 2, 2008. Online at http://www.pcworld.com/printable/article/id,125759/printable.html

Andrle, J.D. (2006). A Winning Hand: A Proposal for an International Regulatory Schema with Respect to the Growing Online Gambling Dilemma in the United States. *UNLV Gaming Research & Review Journal, 10*(1), 59-93.

Angerman, A. (2008). *Is there integrity in online poker?* Retrieved March 23, 2008. Online at http://www.pokerpages.com/articles/archives/angerman03.htm

Anon (2004). "More on Gold Coast Phishing, Gambling Extortion," September 24. Retrieved from www.loosewire.typepad.com/blog. January 25, 2006.

Arkin, B., Hill, F., Marks, S., Schmid, M., Walls, T.J. & McGraw, G. (1999). *How We Learned to Cheat in Online Poker: A Study in Software Security*. Retrieved March 10, 2007.

Arthur, C. (1997). *Suckers Pour Cash into Casino Ripoffs Online*. The Independent (London). pg. 7.

Barker, T., Jones, S., & Britton, C. (1996). An Introduction to Grounded Theory. Retrieved December 26, 2007. Online at http://homepages.feis.herts.ac.uk/~comqtb/Grounded_Theory_intro.htm

Barrett, R. (2004). *Show Me the Money: Foreign Lottery Scams Hit the Jackpot in the U.S.*. Retrieved March 24, 2008. Online at http://www.consumerwebwatch.org/dynamic/fraud-investigation-show-me-the-

money.cfm

Baudrillard, J. (1988). Simulations and Simulacra. In M. Poster, (Ed.), *Jean Baudrillard, Selected Writings* (pp. 166-184). California: Stanford University Press.

Bayne, S. (2004). Smoothness and Striation in Digital Learning Spaces. *E-Learning, 1*(2), 302-316.

(BBC) British Broadcasting Corporation (2007). *Cyber crime tool kits go on sale.* Retrieved March 23, 2008. Online at http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6976308.stm

(BCPRG) British Columbia Partnership for Responsible Gambling (2004). *Internet Gambling.* Retrieved March 20, 2007. Online at http://www.bcresponsiblegambling.ca/other/internet.html

Bednarski, G. (2004). *Enumerating and Reducing the Threat of Transnational Cyber Extortion against Small and Medium Size Organizations.* Retrieved September 13, 2005, from Carnegie Mellon University. Online at http://www.andrew.cmu.edu/user/gbednars/InformationWeek CMU_Cyber_Extortion_Study.pdf

Berg, Bruce L. (2001). *Qualitative Research Methods for the Social Sciences.* Massachusetts: Allyn & Bacon.

Best, J. & Luckenbill, D.F. (1982). *Organizing Deviance.* New Jersey: Prentice-Hall, Inc.

Biever, C. (2004). *How zombie networks fuel cybercrime.* NewScientist.com. Retrieved June 5, 2005. Online at http://www.newscientist.com/channel/info-tech/electronic-threats/dn6616

Bogard, W. (1996). *The Simulation of Surveillance: Hypercontrol in Telematic Societies.* Cambridge: Cambridge University Press.

Bogard, W. (2000). Smoothing Machines and the Constitution of Society. *Cultural Studies, 14*(2), 269-294.

Bortz, B. (2008). Linkedln: Bill Bortz. Retrieved April 4, 2008. Online at http://www.linkedin.com/pub/4/1BB/653

Brenner, S.W. (2001). Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law. Retrieved January 20, 2007. Online at http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html

Brenner, S. W. (2002). Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law &*

Technology, 4(1), 1-41.

Brothersoft.com (2008).Download POD, POD 1.1 Download. Retrieved February 28, 2008. Online at http://www.brothersoft.com/pod-69549.html

Brunker, M. (2004). Poker 'bots' raking online pots? Retrieved March 20, 2008. Online at http://www.msnbc.msn.com/id/6002298/print/1/displaymode/1098/

Bullough, O. (2004). *Police Say Russian Hackers are Increasing Threat.* Retrieved April 5, 2008. Online at http://www.usatoday.com/tech/news/internetprivacy/2004-07-28-russian-hackers_x.htm

Cabot, A. (2001). *Internet Gambling Report IV (4th edition).* Las Vegas: Trace Publications.

Caray, H. (2006). *Nigerian Crooks Pleaded Guilty on Identity Theft Scam with BETonSPORTS Database.* Retrieved April 3, 2008. Online at http://www.sportshandicappingforum.com/showthread.php?t=56569

Casinomeister (2005). *Gambling Federation Casinos.* Retrieved April 2, 2008. Online at http://www.casinomeister.com/rogue/blunders/gamblingfederation.php

Casinomeister (2007). *Absolute Poker – Cheating Poker Room.* Retrieved March 23, 2008. Online at http://www.casinomeister.com/rogue/absolute_poker.php

Cassavoy (2005). *Web of crime: internet gangs go global.* Retrieved October 25, 2005. Online at www.PCWorld.com/news/article

(CCRC) Computer Crime Research Center. (2005). *U.S. Cyber-Crime Unit Focuses on Russian Hackers.* Retrieved May 21, 05. Online at http://crime-research.org/analytics/1226

(CERT-LEXSI) Computer Emergency Response Team - Laboratoire d'EXpertise en Sécurité Informatique (2006). *Online Gaming Cybercrime: CERT-LEXSI'S White Paper*, July 2006.

Chambliss, W. J. (1978). *On the Take: From Petty Crooks to Presidents.* Indiana University Press.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law, 24.* p. 229-251.

Chen, Y.C., Chen, P.C., Hwang, J.J., Korba, L., Song, R. & Yee, G. (2005). An Analysis of Online Gaming Crime Characteristics. *Internet Research, 15*(3), 246-261.

Clarke, D. (2003). Gambling and the trait of addiction in a sample of New Zealand university students. *New Zealand Journal of Psychology, 32*(1), 39-48.

Clarke, R. & Dempsey, G. (2001). The Feasibility of Regulating Gambling on the Internet *Managerial and Decision Economics, 22*(1-3), p. 125-132.

Clinard, M.B. & Quinney, R. (1973). *Criminal Behavior Systems*. New York: Holt, Rinehard Winston.

Cody, J. (2001). *Super Bowl Kicks Off Storm of Illegal Betting*. Times Herald, A-Section, Pg. 1A.

Conte, J. (1997). The Smooth and the Striated: Compositional Texture in the Modern Long Poem. *Modern Language Studies, 27*(20), p. 57-72.

Costigan, C. (2007). *Online Gambling: Hacking by Costa Rican Employees Not Uncommon*. Retrieved March 23, 2008. Online at http://www.gambling911.com/online-gambling-102007.html

Council of Europe. (2004). *Summary of the Organized Crime Situation Report 2004: Focus on the Threat of Cybercrime*. Retrieved on October 15, 2005. Online at http://www.coe.int/T/E/Legal_affairs/Legal_cooperation/Combating_economic_crime/Organised_crime/Documents/OrgCrimeRep2004Summ.pdf

Craven, P. (2007). Google's Crawl Explained. Retrieved December 27, 2007. Online at http://www.webhostdir.com/news/articles/shownews.asp?id=22249

Cressey, D.R. (1969). *Theft of the Nation: The Structure and Operations of Organized Crime in America*. New York: Harper & Row, Pub.

Cressey, D.R. (1972). *Criminal Organization: Its Elementary Forms*. New York: Harper & Row, Pub.

CryptoLogic. (2001). *Update Conference Call*. Retrieved March 20, 2008 from CryptoLogic Inc. Online at http://www.cryptologic.com/pdf/conference_calls/cc_2001_oct9.pdf

Dantzker, M.L. & Hunter, R.D. (2006). *Research Methods for Criminology and Criminal Justice – 2nd edition*. MA: Jones and Bartlett Publishers.

DarkAge. (n.d). *Toolkit*. Retrieved March 23, 2008. Online at http://www.darkage.co.uk/rpg/computers/toolkit.htm

Datz, T. (2004). *Out of Control*. Retrieved March 8, 2006. Online at http://www.csoonline.com/read/080104/control.html

Deleuze, G. & Guattari, F. (1987). *A Thousand Plateaus: Capitalism and Schizophrenia.* Minneapolis: University of Minnesota Press.

Denning, D. (2000). Cyberterrorism. Retrieved October 20, 2007. Online at http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc

Derevensky, J., Gupta, R., & Magoon, M. (2004). Adolescents problem gambling: Legislative and policy decisions. *Gambling Law Review, 8*(2), 107-117.

Dewar, L. (2001). Regulating Internet Gambling: The Net Tightens on Online Casinos and Bookmakers. *Aslib Proceedings, 53*(9). Retrieved March 26, 2007. Online at http://www.emeraldinsight.com/Insight/ViewContentServlet?Filename=Published/EmeraldAbstractOnlyArticle/Pdf/2760530902.pdf

(DOJ) Department of Justice. (2006). *Money Laundering Indictment Unsealed Against Major Internet Gambling Site Operators, Alleges $250 Million In Online Wagers.* Retrieved April 2, 2008. Online at http://www.usdoj.gov/opa/pr/2006/May/06_crm_298.html

DOJ. (2007). *Man Sentenced to 34 Months in Prison for Involvement in Large Identity-Theft Ring.* Retrieved April 3, 2008. Online at http://newyork.fbi.gov/dojpressrel/pressrel07/identitytheft012407.htm

Duff, L., & Gardiner, S. (1996). Computer crime in the global village: Strategies for control and regulation- in defence of the hacker. *International Journal of the Sociology of Law, 24*, p. 221-228.

Einstadter, W. J. (1969). The Social Organization of Armed Robbery. *Social Problems, 17*, 64-83.

Einstadter, W. & Henry, S. (1995). *Criminological Theory: An Analysis of its Underlying Assumptions.* Fort Worth, TX: Harcourt, Brace and Company.

elGordo.com (2008). *Advice About Scams.* Retrieved April 4, 2008. Online at http://www.elgordo.com/info/scamsen.asp

Emigh, A. (2005). *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures.* ITTC Report on Online Identity Theft Technology and Countermeasures. Retrieved March 20, 2007. Online at http://www.savemyos.com/organization/Additinal_PDF_files_files/Phishing-dhs-report.pdf

Eskes, O. (1996). *Bridge in the 21st century.* Retrieved March 21, 2008. Online at http://www.imp-bridge.nl/articles/okb.htm

Euromilliones.com (2006). *Attention Scam Letters & Emails.* Retrieved April 23, 2008.

Online at http://www.euromillones.com/scams_euromillions.asp

Fabiansson, C. (2006). Social cohesion and leisure activities – Youths' gambling experiences. *Journal of Youth Studies*, *9*(3), 345–360.

(FACC) Forum d'Action des Communautes Culturelles. (n.d.). *Internet Gambling.* Retrieved April 2, 2008. Online at http://www.facc.ca/Publication/anglais/Internet%20gambling.htm#_edn11

(FinCEN) Financial Crimes Enforcement Network. (1998). *Suspicious Activity Reporting and Casinos*. Retrieved October 12, 2006. Online at http://www.fincen.gov/sarcasin.html

Gambling.co.uk (2006). *BOS Argentina Hacked By Punters*. Retrieved March 23, 2008. Online at http://www.gamblog.co.uk/2006_08_01_archive.htm

Gambling Magazine. (1999). *The Real Danger for This Industry*. Retrieved October 19, 2006. Online at http://gamblingmagazine.com/articles/starnet/starnet113.htm

GamCare. (2004). *Children as Young as 11 Can Set Up Gambling Accounts at the Click of a Button*. Retrieved March 28, 2007. Online at http://www.gamcare.org.uk/pdfs/PressreleaseFinal.pdf

(GAO) General Accounting Office. (2002). *Internet Gambling: An Overview of the Issues*. Report to Congressional Requesters, December 2002. Retrieved November 14, 2007. Online at http://www.gao.gov/new.items/d0389.pdf

Gaudin, S. (2004). *SoBig's Birthday – Tracking Most Damaging Virus Ever*. Retrieved April 5, 2008. Online at http://itmanagement.earthweb.com/secu/article.php/3297551

Genosko, G. (2001). *Deleuze and Guattari: Critical Assessments of Leading Philosophers, Volume III*. London: Routledge.

Germain, Jack M. (2003). Computer Viruses and Organized Crime: The Inside Story. Retrieved November 10, 2005. Online at http://www.technewsworld.com/story/31679.html

Germain, Jack M. (2004). *Global Extortion: Online Gambling and Organized Hacking.* Retrieved May 21, 2005, from Mac News World. Online at http://www.macnewsworld.com/story/33171.html

Gibbons, D.C. (1977). *Society, Crime, and Criminal Careers*. New Jersey: Prentice-Hall.

Gilad. (2007). *Josh "JJProdigy" Fields Asks Poker World For Forgiveness*. Retrieved

April 3, 2008. Online at http://www.tightpoker.com/news/Josh-JJProdigy-Fields-Asks-Forgiveness.shtml

Glavan, D. (2003). *Russian Hackers Raid Largest Online Gaming Operation and Destroy Data in Blackmail.* Retrieved April 5, 2008. Online at http://www.xatrix.org/article.php?s=2726

Goelle, P. & Ducheneaut, N. (2005). Preventing Bots from Playing Online Games. *ACM* Computers in Entertainment, 3(3), 1-10.

Goldman, R. (2007). *Online Poker Players Expose Alleged Fraud.* Retrieved January 29, 2008. Online at http://abcnews.go.com/print?id=3752500

Goldsmith, J. (n.d.). *Report from OKBridge C&E Commitee (ki case).* Retrieved March 21, 2008. Online at http://www.gg.caltech.edu/~jeff/kireport

Golubev, V. (2005). *DoS attacks: crimes without penalty.* Retrieved June 5, 2005, from Computer Crime Research Center (CCRC). Online at http://www.crime-research.org/articles/1049/

Goodell, J.(1996). *The cyber thief and the samurai.* New York: Dell Publishing.

Goodman, M.D. (1997). Why the Police Don't Care About Computer Crime. *Harvard Journal of Law and Technology, 10,* 465-494.

Goodson, P., McCormick, D. & Evans, A. (2001). Searching for Sexually Explicit Materials on the Internet: An Exploration of College Students' Behaviour and Attitudes. *Archives of Sexual Behaviour 30.* p. 104-118.

(GoogleTech) Google Technology (2008). Google Searches More Sites More Quickly, Delivering the Most Relevant Results. Retrieved December 27, 2007. Online at http://www.google.com/technology/

Gray, P. (2005). *Hackers: The Wind of Change.* Retrieved June 5, 2005. Online at http://www.iss.net/newsletters/secured/mar2005/winds_of_change.php

Griffiths, M. (1994) The role of cognitive bias and skill in fruit machine gambling. *British Journal of Psychology 85,* 351–369.

Griffiths, M. (2003). Internet Gambling: Issues, Concerns, and Recommendations. *CyberPsychology & Behavior, 6*(6), 557-568.

Griffiths, M. (2006). Adolescent gambling on Category D machines, excessive gambling and addiction. *Report prepared for the Gambling Commission.* Retrieved on June 1, 2007. Online at http://www.gamblingcommission.gov.uk/UploadDocs/Misc/sop_responses/

Mark%20Griffiths.pdf

Griffiths, M.D. & Wood, R.T.A. (2000). Risk factors in adolescence: The case of gambling, video game playing and the internet. *Journal of Gambling Studies, 16*, 199-225.

(GRP) Golden Rule of Poker (1999).*Gambling Malware and Gambling Spyware.* Retrieved April 2, 2008. Online at http://www.goldenruleofpoker.com/spyware-and-malware.htm

Gu, Q., Liu, P. & Chu, C. (2004). Hacking Techniques in Wired Networks. Retrieved March 23, 2008. Online at http://ist.psu.edu/s2/paper/hack-wired-network-may-04.pdf

Hafner, K., & Markoff, J. (1995). *Cyberpunks: Outlaws and hackers on the computer frontier*. Toronto: Simon and Schuster.

Hagan, Frank E. (1994). *Introduction to Criminology.* Illinois, Chicago: Nelson-Hall Inc.

Hamman, R.B. (1996). Rhizome@Internet: Using the Internet as an Example of Deleuze and Guattari's "Rhizome". Retrieved May 24, 2007. Online at http://www.socio.demon.co.uk/rhizome.html

Heinrichs, P. (2001). *Beware of the Dot Con Artists*. The Sunday Age, pg.6.

Herman, A. & Sloop, J. (2000). 'Red Alert!': rhetorics of the world wide web and 'friction free' capitalism', in A. Herman & J. Sloop, *The World Wide Web and Contemporary Cultural Theory*. London: Routledge.

Hill, B. (2004). Timing Google's Crawl. Retrieved December 27, 2007. Online at http://www.dummies.com/WileyCDA/DummiesArticle/Timing-Google-s-Crawl.id-2555.html

Hodgson, N.& Standish, P. (2006). Induction into Educational Research Networks: The Striated and the Smooth. *Journal of Philosophy of Education, 40*(4), p 563-574.

HoldemGenius (2008a). *Texas Hold'em Odds Calculator - Get Texas Hold'em Odds with Holdem Genius*. Retrieved April 2, 2008. Online at http://www.holdemgenius.com

HoldemGenius (2008b). *Holdem Genius™ Screenshots*. Retrieved April 2, 2008. Online at http://www.holdemgenius.com/screenshots.html

HoldemGenius (2008c). *Software Updates - Holdem Genius*. Retrieved April 2, 2008. Online at http://www.holdemgenius.com/software-updates.html

HoldemGenius (2008d). *Contact Us - Holdem Genius*. Retrieved April 2, 2008. Online at http://www.holdemgenius.com/contact.html

Ianni, F.A. (1974). *Black Mafia: Ethnic Succession in Organized Crime*. New York: Simon & Schuster.

(IGDA) International Game Developers Association. (2004). *2004 Web and Downloadable Games White Paper*. Presented at the Game Developers Conference 2004 by the IGDA Online Games SIG. Retrieved September 10, 2006. Online at http://www.igda.org/online/IGDA_WebDL_Whitepaper_2004.pdf

IndianExpress (2008). *Nigerian, two others arrested for 'online lottery fraud'*. Retrieved March 24, 2008. Online at http://www.expressindia.com/latest-news/Nigerian-two-others-arrested-for-online-lottery-fraud/263514/

Isachenkov, V. (2004). *Russian Hackers Extort Cash From British Bookmakers*. Retrieved April 5, 2008. Online at http://www.informationweek.com/shared/printableArticle.jhtml?articleID=26100601

(ITU) International Telecommunication Union. (2008). *ITU Botnet Mitigation Toolkit*. Retrieved March 23, 2008. Online at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf

Jellenc, E. & Zenz, K. (2007). Global Threat Research Report: Russia. Retrieved October 11, 2007. Online at http://www2.csoonline.com/whitepapers/Verisign62607.pdf

Jepson, V. (2000). Internet Gambling and the Canadian Conundrum. *Appeal Review of Current Law and Law Reform, 6*(6), 6-13.

Jewkes, Y. (2007). *Crime Online: Committing, Policing, and Regulating Crime*. Oregan: Willan Publishing.

Jones, S.G.(1995). *Cybersociety: Computer-mediated Communication and Community*. Thousand Oaks, CA: Sage

Jordan, T. & Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review, 46*(4), 757-780.

Karshmer, A. (2005). *Virtual Villains: Global Gangsters are extorting money from online casinos with a novel threat: we'll spam you to death.* Retrieved September 13, 2005, from MSNBC. Online at http://msnbc.msn.com/id/5505593/site/newsweek/

Keller, B.P. (1999). The Game's the Same: Why gambling in Cyberspace Violates Federal Law. *The Yale Law Journal, 108*(7), 1569-1609.

Kelley, L. (1997). *Betting With Internet Casinos Can Be A Real Roll of the Dice.* Retrieved March 23, 2007, from the Sun-Sentinal.com. Online at http://pqasb.pqarchiver.com/sun_sentinel/access/13970437.html?dids=13970437:13970437&FMT=ABS&FMTS=ABS:FT&date=Sep+8%2C+1997&author=LANE+KELLEY+Staff+Writer&pub=Sun+Sentinel&edition=&startpage=1.A&desc=BETTING+WITH+INTERNET+CASINOS+CAN+BE+A+REAL+ROLL+OF+THE+DICE

Kelley, R., Todosichuk, P. & Azmier, J.J. (2001). *Gambling @ Home: Internet Gambling in Canada.* Canada West Foundation, Gamblin g in Canada Research Report No. 15.

(KGC) Kahnawá:ke Gaming Commission (2008). In the Matter of Absolute Poker: Investigation Regarding Complaints of Cheating.

Kilger, M., Arkin, O. & Stutzman, J. (2004). *Profiling.* Retrieved October 31, 2007. Online at http://searchsecurity.techtarget.com/searchSecurity/downloads/Honeynet_Ch16.pdf

Kish, S. (1999). Betting on the Net: An Analysis of the Government's Role in Addressing Internet Gambling. *Federal Communications Law Journal, 51*(2), 449-466.

Korn, D.A. (2000). Expansion of gambling in Canada: Implications for health and social policy. *Canadian Medical Association Journal, 163*, 61–64.

Kowalski, M. (2002). *Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics.* Retrieved April 18, 2007. Online at http://www.statcan.ca/english/freepub/85-558-XIE/85-558-XIE2002001.pdf

Krone, Tony. (2005). *Hacking Motives.* Retrieved March 8, 2006. Online at http://www.aic.gov.au/publications/htcb/htcb006.pdf

Kvarnstrom,H., Lundin, E. & Jonsson, E. (2000). *Combining Fraud and Intrustion Detection – Meeting New Requirements.* Retrieved March 10, 2007. Online at http://www.ce.chalmers.se/~emilie/papers/Kvarnstrom_nordsec2000.pdf

Ladd, G.T. & Petry, N.M. (2002): Gender differences among pathological gamblers seeking treatment. *Experimental and Clinical Psychopharmacology 10*, 302-309.

LeBeuf, Marcel-Eugene. (2001). *Organized Crime and Cybercrime: Criminal Investigations on the Cutting Edge.* Retrieved December 1, 2005, from Canadian Policing College. Online at http://www.cpc.gc.ca/research/ocrime_e.pdf

Lemieux, V. (2003). *Criminal Networks.* Retrieved January 14, 2006, from RCMP. Online at http://www.rcmp.ca/ccaps/reports/criminal_net_e.pdf

Levitt, S. D. (2007). The Absolute Poker Cheating Scandal Blown Wide Open. Retrieved January 29, 2008. Online at http://freakonomics.blogs.nytimes.com/2007/10/17/the-absolute-poker-cheating-scandal-blown-wide-open/

Light, A. & Smith, J.M. (1998). *Philosophy and Geography III: Philosophies of Place.* Maryland: Rowman & Littlefield Publishers, Inc.

Lilley, P. (2003). Dirty Dealing: The Untold Truth about Global Money Laundering, International Crime and Terrorism. London: Kogan Page Ltd.

Littman, J. (1995). *The fugitive game: online with Kevin Mitnick.* Toronto: Little Brown & Company.

Lort, R. (2000). *Rhizomatic Ontologies.* Retrieved January 3, 2008. Online at http://members.optusnet.com.au/~robert2600/azimute/texts/rhizomatic_ontologies.html

Lyman, M. D. & Potter, G. W. (1997). *Organized Crime.* New Jersey: Prentice-Hall Inc.

Makela, C. J., (2000). Youth gambling: A consumer issue. *Consumer Interests Annual 46*, 218.

Mann, C. & Stewart, F. (2004). Introducing Online Methods. In S.N. Hesse-Biber, & P. Leavy (Eds.), Approaches to Qualitative Research: A Reader on Theory and Practice (pp. 367-401). Oxford University Press.

Mann, D. & Sutton, M. (1998). Netcrime: More Change in the Organization of Thieving. *British Journal of Criminology, 38*, p. 201-229.

Mark, R. (2007). *BetonSports ID Thief Sentenced to 34 Months.* Retrieved April 3, 2008. Online at http://www.insideid.com/print.php/3656181

Mars, G. (2000). Culture and Crime. In D. Canter and L. Alison, (Eds.), *The Social Psychology of Crime: Groups, Teams and Networks* (pp. 23-50). England: Ashgate Publishing Company.

Mason, J. (2002). *Qualitative Researching - 2nd edition.* London: Sage Publications Inc.

McAfee. (2005). *McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet.* Retrieved October 20, 2005. Online at http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf

McAfee (2006). *Rootkits, Part 1 of 3: The Growing Threat.* Retrieved November 3, 2007. Online at

http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_akapoor_rootkits1_en.pdf

McAfee (2007). *McAfee North America Criminology Report: Organized Crime and the Internet 2007.* Retrieved January 21, 2008. Online at http://us.mcafee.com/en-us/local/html/identity_theft/NAVirtualCriminology Report07.pdf

McAndrew, D. (2000). The Structural Analysis of Criminal Networks. In D. Canter and L. Alison, (Eds.), *The Social Psychology of Crime: Groups, Teams and Networks* (pp. 53-94). England: Ashgate Publishing Company.

McDowell, J. & Novis, G. (2001). *The Consequences of Money Laundering and Financial Crime.* Retrieved March 8, 2006, from U.S Department of State. Online at http://usinfo.state.gov/journals/ites/0501/ijee/state1.htm

McGeathy, J. (2001). Keeping Things Secure. In A. Cabot, *Internet Gambling Report IV (4th edition)* (121-132). Las Vegas: Trace Publications.

McGraw, G. & Hoglund, G. (2007). Chapter 2: Game Hacking 101, from Exploiting Online Games: Cheating Massively Distributed Systems. Addison-Wesley Professional. Retrieved March 20, 2008. Online at http://www.informit.com/content/images/9780132271912/samplechapter/0132271915_CH02.pdf

McIntosh, M. (1975). *The Organization of Crime.* London: Macmillan.

McMillen, J. & Grabosky, P. (1998). Internet Gambling. *Australian Institute of Criminology: Trends & Issues in Crime and Criminal Justice, 88.*

McMullan, J. L. & Perrier, D. C. (2003). Technologies of Crime: The Cyber-Attacks on Electronic Gambling Machines. *Canadian Journal of Criminology and Criminal Justice, 45*(2), 159-186.

McMullan, J. & Rege, A. (2007). *Cyberextortion at Online Gambling Sites: Criminal Organization and Legal Challenges. Gaming Law Review, 11*(6), 648-665.

Meerkamper, E. (2006). Decoding Risk: Gambling Attitudes and Behaviours Amongst Youth in Nova Scotia. *Nova Scotia Gaming Corporation.*

Michalowski, R., & Pfuhl, E. (1991). Technology, property and law: The case of computer crime. *Crime, Law and Social Change, 15*, p. 255-275.

(MIL) McConnell International LLC. (2000). Cybercrime...*and Punishment? Archaic Laws Threaten Global Information.* Retrieved October 21, 2005. Online at http://www.iwar.org.uk/law/resources/cybercrime/mcconell/CyberCrime.pdf

Mitka, M. (2001). Win or lose, Internet gambling stakes are high. *Journal of the American Medical Association, 285,* 1005.

Mitnick, K.D. and W.L. Simon (2005). *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders and Deceivers.* New York: Wiley.

Morgan, G. (2005). *Locked Out: A growing band of extortionists, political activists and malevolent hackers are using denial of service attacks to overwhelm and close down online businesses and public sector web sites.* Retrieved November 10, 2005, from Infoconomy. Online at http://www.infoconomy.com/pages/recent-management-articles/group107079.adp

Morse, E. (2006). Extraterritorial Internet Gambling: Legal Challenges and Policy Options. *Social Science Research Network (SSRN).*

Moulthrop. (1994). Rhizome and Resistance: Hypertext and the Dreams of a New Culture, in G. Landlow (Ed.) *Hyper/text/theory.* Baltimore: John Hopkins University Press.

Murphy, A., Pender, A., Reily, L., & Connel, S. (2005). *Denial of Service and Countermeasures.* Retrieved May 21, 05, from Networks and Telecommunications Research Group. Online at http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group2/

Myers, M. (1995). Deleuze-Guattari discussion list. Retrieved June 5, 2007. Online at http://www.gpc.edu/~mnunes/smooth.html

Naraine, R. (2006). *Rootkit Infiltrates Online Poker Software.* Retrieved March 21, 2008. Online at http://www.eweek.com/c/a/Security/Rootkit-Infiltrates-Online-Poker-Software/

Neuman, L. W. (2003). *Social Research Methods: Qualitative and Quantitative Approaches.* Massachusetts: Allyn & Bacon.

NorthCountryGazette (2006). Massive Internet Gambling Operation Busted. Retrieved March 20, 2008. Online at http://ww.northcountrygazette.org/articles/111506InternetGambling.html

Nunes, M. (1999). Virtual Topographies: smooth and striated cyberspace, in M.L. Ryan (Ed.) *Cyberspace Textuality: computer technology and literary theory.* Bloomington: Indian University Press.

O'Brien, T.L. (2000). *Aided by Internet, Identity Theft Soars.* The New York Times. Retrieved March 20, 2007. Online at http://www.personal.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/IDtheft.

pdf

Oldenburg, R. (1989). *The Great Good Place: Cafes, Coffee Shops, Community Centers, Beauty Parlors, General Stores, Bars, Hangouts, and How They Get You Through the Day*. New York: Paragon House.

Online-Casinos (2008). *DDOS Danger for Online Gambling Sites*. Retrieved April 3, 2008. Online at http://www.online-casinos.com/news/news6272.asp

OnlinePoker-News.com (2007). Bots are Used to Launder Money in Online Casinos. Retrieved March 20, 2008. Online at http://www.onlinepoker-news.com/20070906/bots_are_used_to_launder_money_in_online_ich.aspx

Paccagnella, L. (1997). Getting the seat of your pants dirty: Strategies for ethnographic research on virtual communities. *Journal of Computer-Mediated Communication, 3*(1). Retrieved March 2, 2007. Online at http://jcmc.indiana.edu/vol3/issue1/paccagnella.html

Parke, J., Rigbye, J., Parke, A., & Williams, L. V. (2007). eCOGRA Global Online Gambler Report: An Exploratory Investigation into the Attitudes and Behaviours of Internet Casino and Poker Players. *e-Commerce and Online Gaming* Regulation and Assurance (eCOGRA).

Patton, P. (2000). *Deleuze and the Political*. London: Routledge.

Paulson, R.A. & Weber, J.E. (2006). Cyberextortion: An Overview of Distributed Denial of Service Attacks Against Online Gaming Companies. *Issues in Information Systems, 7*(2), 52-56.

Payton, A. (2005). *Determining the Proper Response to Online Extortion*. Paper presented at the Information Security Curriculam Development Conference, September 23-24, 2005.

(PBS) Public Broadcasting Service (2001a). *Interview: Raphael gray a.k.a. curador*. Retrieved October 15, 2007. Online at http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/curador.html

PBS (2001b). *Interview: anonymous*. Retrieved October 15, 2007. Online at http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/anon.html

PBS (2001c). *Interview: Bruce Schneier*. Retrieved October 15, 2007. Online at http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/anon.html

PBS (2001d). *Interview:Chris Davis*. Retrieved October 15, 2007. Online at

http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/davis.html

Penenberg, A.L. (1998). *Gambler Beware*. Retrieved March 26, 2007, from Forbes Digital Tool: E-Business. Online at http://www.gaminglinks.com/articles/forbes/feat.htm

PolicyHub. (2007). How Do You Know Why (and How) Something Works? Retrieved December 27, 2007. Online at http://www.policyhub.gov.uk/evaluating_policy/magenta_book/chapter8b.asp

Poster, M. (1995). Databases as Discourse, or Electronic Interpellations, in *The Second Media Age*. Polity Press.

Pregame.com (2006). *BetonSports: The World is Yours*. Retrieved March 23, 2008. Online at http://www.pregame.com/forums/forums/p/1823/6376.aspx

Prus, R. (2004). Gambling as activity: Subcultural life-worlds, personal intrigues and persistent involvements. *The Electronic Journal of Gambling Issues.* Issue10.

PRNewsWire. (2001). *MaxLotto Officially launches world's biggest continuous lottery in Britain With 69.3 Million Pounds Sterling Biweekly Jackpot and 6.93 Million pounds weekly jackpot*. Retrieved April 4, 2008. Online at http://www.prnewswire.co.uk/cgi/news/release?id=63585

Queen, L. (2007). *Smart Scarborough senior avoids lottery scam*. Retrieved April 4, 2008. Online at http://www.insidetoronto.ca/News/Scarborough/article/30128

Ranade, S., Bailey, S., & Harvey, A. (2006). *A Literature Review and Survey of Statistical Sources on Remote Gambling*. Retrieved November 1, 2006. Online at http://www.culture.gov.uk/NR/rdonlyres/E0A395C1-35CC-4717-BF00-B1F6BD3A6B76/0/RemoteGambling_RSeReport.pdf

Ratliff, E. (2005). *The Zombie Hunters: On the Trail of Cyberextortionists.* Retrieved December 5, 2005. Online at http://www.newyorker.com/printables/fact/05101fa_fact

(RCMP) Royal Canadian Mounted Police. (2007). *Integrated Technology Crime Unit (ITCU)*. Retrieved July 3, 2007. Online at http://www.rcmp-grc.gc.ca/on/prog_serv/support_serv/itcu_e.htm

(Reuters) Reuters News Service (2001). *Hackers Win High Stakes at Gambling Sites*. Retrieved April 25 2005. Online at *CNET news.com*

Reuter, P. (1983). *Disorganized Cirme: The Economics of the Visible Hand*. MA: MIT Press.

Rheingold, H. (1993). *The Virtual Community: Homesteading on the Electronic Frontier.* MA: Addison-Wesley.

Rogers, M.K. (2005). *The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach.* Retrieved January 23, 2007. Online at https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2005-43.pdf

Rosencrance, L. (2003). Cyberscam Strikes Massachusetts State Lottery. Retrieved January 29, 2008. Online at http://www.computerworld.com/printthis/2003/0,4814,82892,00.html

Schloenhardt, A. (1999). *Organised Crime and the Business of Migrant Trafficking – An Economic Analysis.* Retrieved December 20, 2005. Online at http://www.aic.gov.au/conferences/occasional/schloenhardt.pdf

Schwartau, W. (2000). *Cybershock: Surviving hackers, phreakers, identity thieves, internet terrorists and weapons of mass destruction.* New York: Thunder Mouth Press.

Shaffer, H.J (1996) Understanding the Means and Objects of Addiction: Technology, the Internet, and Gambling. *Journal of Gambling Studies 12*(4), 461–469.

Shaw, C. (2004). *Net Surfing More Than Working? Websense Cuts Down On Misuse.* Investor's Business Daily, National Edition, Pg. B02.

Shoemaker, P., Tankard Jr., J., Lasorsa, D. (2004). *How to Build Social Science Theories.* California: Sage Publications, Inc.

Shover, N., Coffey, G.S. & Hobbs, D. (2003). Crime on the Line: Telemarketing and the Changing Nature of Professional Crime, *British Journal of Criminology 43*, p. 489-506.

Skidmore, W. (1975). *Theoretical Thinking in Sociology.* New York: Cambridge University Press.

Skoudis, E. (2007). *What are the Risks or Logging into a Botnet Control Channel?* Retrieved October 31, 2007. Online at http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1274217,00.html

Smeaton, M. & Griffiths, M. (2004). Internet Gambling and Social Responsibility: An Exploratory Study. *CyberPsychology & Behavior, 7*(1), 49-57.

Smed, J., Knuutila, T. & Hakonen, H. (2006). *Can We Prevent Collusion in Multiplayer Online Games?* Retrieved January 10, 2007. Online at

http://www.stes.fi/scai2006/proceedings/168-175.pdf

Smith, D.C. (1974). *The Mafia Mystique*. New York: Basic Books.

Smith, R. (2003). *Investigating Cybercrime: Barriers and Solutions*. Retrieved July 3, 2007. Online at http://www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf

SmokePoker.com (2008). Free Poker Bot – Instant Download! Retrieved March 20, 2008. Online at http://smokepoker.com

(SNJCI & AGNJ) State of New Jersey Commission of Investigation & Attorney General of New Jersey. (2000). *Computer Crime: A Joint Report.* Retrieved March 26, 2007. Online at http://csrc.nist.gov/publications/secpubs/computer.pdf

Speer, D. L. (2000). Redefining Borders: The Challenges of Cybercrime. *Crime, Law and Social Change, 34*, 259-273.

(SPI) Silverthorne Publications, Inc. (2006a). *Online Gambling Toolkit Order Form.* Retrieved April 2, 2008. Online at http://www.onlinegamblingtoolkit.com/order.htm

(SPI) Silverthorne Publications, Inc. (2006b). *Online Gambling Toolkit*. Retrieved April 2, 2008. Online at http://www.onlinegamblingtoolkit.com

Stewart, D.O. (2006). *An Analysis of Internet Gambling and its Policy Implications.* American Gambling Association's series of 10th anniversary White Papers.

Sturgeon, W. (2005). *Online gamblers targeted by scams*. Retrieved March 26, 2007. Online at http://news.com.com/Online+gamblers+targeted+by+scams/2100-7349_3-6073880.html

Sullivan, D. (2007). *Botnets Meet Ocean's Eleven: Scamming Online Gambling.* Retrieved April 2, 2008. Online at http://www.realtime-websecurity.com /articles_and_analysis/2007/10/botnets_meet_oceans_eleven_sca.html

Swartz, J. (2004). *Crooks slither into Net's shady nooks and crannies*. Retrieved October 19, 2005. Online at www.USAtoday.com/tech/news

Swenson, D. (1999). *How to Evaluate a Theory*. Retrieved April 25, 2008. Online at http://faculty.css.edu/dswenson/web/theoryeval.html

Symantec (2000). *Learn More About Viruses and Worms*. Retrieved November 3, 2007. Online at http://www.symantec.com/avcenter/reference/worm.vs.virus.pdf

Symantec (2007a).*What is Cybercrime?* Retrieved July 3, 2007. Online at

http://www.symantec.com/avcenter/cybercrime/index_page2.html

Symantec (2007b). *Symantec Internet Security Threat Report: Trends for January-June 2007*. Retrieved October 31, 2007. Online at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent_whitepaper_internet_security_threat_resport_xii_09_2007.en-us.pdf

Taylor, M., Holland, G. & Quayle, E. (2001). Typology of Paedophile Picture Collections. *The Police Journal*, 74. p. 97-107.

TheGames (2007). *The games * The source of casino insiders!* Retrieved April 2, 2008. Online at http://thegamest.com/thegames_news_15206.html

Thompson, C. (2004). *The Virus Underground.* Retrieved April 5, 2008. Online at http://www.nytimes.com/2004/02/08/magazine/08WORMS.html?pagewanted=8&ei=5007&en=a92a0363448a40de&ex=1391576400&partner=USERLAND

Thompson, I. (2007). Phishing Attacks Target PartyPoker. Retrieved March 20, 2008. Online at http://www.vnunet.com/vnunet/news/2183974/phishing-attack-targets-party

TimesOfIndia (2008). *Nigerian Arrested for Online Fraud.* Retrieved April 4, 2008. Online at http://timesofindia.indiatimes.com/Cities/Mumbai/Nigerian_arrested_for_online_fraud/articleshow/2714862.cms

Toscano, P. (2000). *Taming the Cyber-Frontier: Security is Not Enough!* Retrieved February 10, 2007. Online at http://www.stsc.hill.af.mil/crosstalk/2000/11/toscano.html

Tse, S., Abbott, M., Clarke, D., Townsend, S., Kingi, P. & Manaia, W. (2005). Why People Gamble. *Health Research Council of New Zealand.*

Turkle, S. (1997). Multiple Subjectivity and Virtual Community at the End of the Freudian Century. *Sociological Inquiry, 67* (1), 72-83

Turkulainen, J. (2006). *F-Secure Trojan Information Pages: Small.la.* Retrieved March 21, 2008. Online at http://www.f-secure.com/v-descs/small_la.shtml

(USASDNY) United States Attorney Southern District of New York (2005). *U.S. Indicts 17 in Massive Crackdown on Multi-million Dollar Illegal Gambling Operation.* Retrieved September 24, 2007. Online at http://www.usdoj.gov/usao/nys/pressreleases/January05/uvarietalindictmentpr.pdf

(USASDNY) United States Attorney Southern District of New York (2006). *U.S. Announces Guilty Plea in Large and Sophisticated Identity Theft Ring.* Retrieved

April 3, 2008. Online at http://www.usdoj.gov/usao/nys/pressreleases/July06/elekedepleapr.pdf

Venezia, T., Martinez, E. & Livingston, I. (2006). *$3.3 Bil Casino Royale: 'Net Bet King of Qns. In 'Biggest Ever' Bookie Bust.* Retrieved April 2, 2008. Online at http://www.nypost.com/php/pfriendly/print.php?url=http://www.nypost.com/seven/11162006/news/regionalnews/3_3_bil_casino_royale_regionalnews_todd_venezia_____erika_martinez_____ikimulisa_livingston.htm

Wagner, D. (1984). *The Growth of Sociological Theories.* California: Sage Publications, Inc.

Walker, C. (2004). *Russian Mafia Extorts Gambling Websites.* Retrieved November 10, 2005. Online at http://www.americanmafia.com/Feature_Articles_270.html

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age.* UK: Polity Press.

Walters, L.G. (2003). *Gambling Law Update.* Retrieved January 29, 2008. Online at http://www.gamblinglawupdate.com/archives/Gambling%20Update-%20Aug.%202003.pdf

Wang, S.J., & Ke, H. J. (2004). Curbing gambling activities on the Internet. *IEEE Aerospace and Electronic Systems Magazine, 19(*4), p. 33-35.

Warner, B. (2001). *Hackers Heaven: Online Gambling.* Retrieved September 14, 2005, from CBS News. Online at http://www.cbsnews.com/stories/2001/09/10/tech/main310567.shtml

Weaver, N., Paxson, V., Staniford, S. & Cunningham, R. (2003). *A Taxonomy of Computer Worms.* University of Berkley. Retrieved March 8, 2006. Online at http://www.cs.berkeley.edu/~nweaver/papers/taxonomy.pdf

Wenninger, A. (2007). Terriroty(ies) Internet: Deleuzian perspective on ownership and identity on the web. Retrieved November 17, 2007. Online at http://web.mit.edu/comm-forum/mit5/papers/mit5_wenninger.pdf

Westervelt, R. (2007). *Cybercriminals employ toolkits in rising numbers to steal data.* Retrieved October 31, 2007. Online at http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gcil271024,00.html

Whitaker, R. (1999). *The End of Privacy: How Total Surveillance is Becoming a Reality.* New York: The New Press.

Wilding, E. (2006). *Information Risk and Security: Preventing and Investigating*

Workplace Computer Crime. England: Gower Publishing Ltd.

Williams, P. (2002). *Organized Crime and Cybercrime: Synergies, Trends, and Responses.* Retrieved January 19, 2006 from http://crimeresearch.org/library/Cybercrime.htm

Wilson, P. A., & Molander, R. C. (1998). *Exploring Money Laundering Vulnerabilities Through Emerging Cyberspace Technologies*. Retrieved October 8, 2006. Online at http://www.rand.org/pubs/monograph_reports/MR1005/MR1005.ch5.pdf

(WPR) World Poker Rules (2007). Sorel Mizzi & Chris Vaughn: A Dissenting Opinion. Retrieved March 25, 2008. Online at http://www.worldpokerrules.com/news.php?id=368

Wray, S. (2003). *A Thousand Plateaus*. Retrieved May 24, 2007. Online at http://www.thing.net/~rdom/ecd/rhizomatic.html

Yan, J. (2003). *Security Design in Online Games*. Retrieved January 10, 2007. Online at http://homepages.cs.ncl.ac.uk/jeff.yan/acsac03.pdf

Yan, J. & Randell, B. (2005). *A Systematic Classification of Cheating in Online Games.* NetGames'05. Retrieved March 10, 2007. Online at http://www.research.ibm.com/netgames2005/papers/yan.pdf

Yoo, John. (2005). *Fighting the New Terrorism*. Retrieved January 14, 2005, from American Enterprise Institute for Public Policy Research. Online at http://www.aei.org/publications/pubID.22735,filter.all/pub_detail.asp

Youn, S., Wan, F. & Faber, R.J. (2001). "We should censor because they are vulnerable: censorship of controversial web sites and the third-person perception", in Taylor, C.R. (Eds),*The Proceedings of the 2001 Conference of The American Academy of Advertising*, The American Academy of Advertising, p.72-81.

Zacharias, J. (2004). *Internet Gambling: Is It Worth The Risk?*. Retrieved March 20, 2007. Online at http://www.bcresponsiblegambling.ca/other/docs/ internet_gambling_jan_zacharias.pdf

ZDNet (2005). *Russian Hackers 'the Best in the World'*. Retrieved April 5, 2008. Online at http://news.zdnet.co.uk/security/0,1000000189,39193999,00.htm?r=1