Journal Information
Journal ID (publisher-id): jgi
ISSN: 1910-7595
Publisher: Centre for Addiction and Mental Health

Article Information
© 1999-2001 The Centre for Addiction and Mental Health
Received Day: 8 Month: August Year: 2009
Accepted Day: 13 Month: November Year: 2009
Publication date: July 2010
First Page: 54 Last Page: 85
Publisher Id: jgi.2010.24.5
DOI: 10.4309/jgi.2010.24.5

Online crime and internet gambling

John L. McMullan[1]

Aunshul Rege[2]

[1]Department of Sociology and Criminology, Saint Mary's University, Halifax, N.S. Email: john.mcmullan@smu.ca

[2]School of Criminal Justice, Rutgers University, Newark, New Jersey, U.S.A.

This article was peer-reviewed. All URLs were available at the time of submission.

For correspondence: Dr. John L. McMullan, Saint Mary's University, McNally Building, South Wing, Fourth Floor, 923 Robie Street, Halifax, Nova Scotia, B3H 3C3, Canada. Tel: 902-420-5885, Fax: 902-420-5121. E-mail: john.mcmullan@smu.ca

Contributors: JM was responsible for oversight of all the work reported here and had primary responsibility for manuscript preparation and revision. AR collected the data and conducted the initial document analysis.

Competing interests: There were no competing interests for either author.

Ethics approval: Not required.

Funding sources by author: This research was funded by the Social Sciences and Humanities Research Council of Canada and Saint Mary's University. AR used a Social Sciences and Humanities Research Council of Canada Scholarship Award and JM used research monies from Saint Mary's University.

John L. McMullan, PhD, is a professor of sociology and criminology at Saint Mary's University in Halifax, Nova Scotia, Canada. Professor McMullan is the author of eight books, seven government reports, and over 60 academic articles on business crime; criminal organization; law enforcement; media; crime and justice; gambling and advertising; and gambling, crime, and social policy. He is a commissioner of the Law Reform Commission of Nova Scotia and a member of the executive board of the Nova Scotia Criminal Justice Association.

Aunshul Rege, MA, is currently a PhD student at the Rutgers School of

Criminal Justice in Newark, New Jersey, USA. Her interests include Internet gambling and crime, online fraud and identity theft, cybercriminal organization, and cyberoffender rationality. Her PhD research examines cybercrime and critical infrastructure.

Abstract

The spread of Internet gambling has raised several issues concerning motivations to gamble, consumer behaviour online, problem gambling, security of Web sites, and fairness and integrity of the games. Rather surprisingly, however, there has been little in the way of research regarding online crime and Internet gambling even though it is an urgent priority. This article addresses this absence by investigating the types, techniques, and organizational dynamics of online crime at the portals of Internet gambling sites. Our approach is qualitative in nature and explores, using document analysis, the activities of cybernomads, *dot.con* teams, and criminal networks. We demonstrate that there are different levels of criminal organization, distinguished by their complexity of division of labour; coordination of roles; purposefulness of association between criminals; and ability to avoid, evade, or neutralize security systems and law enforcement. We conclude by arguing that conventional understandings of real-world gambling-related criminal relationships have been altered by the digital environment of the Internet.

Introduction

Over the past 14 years there has been a global explosion in online gambling, allowing customers to play 24 hours a day, seven days a week, from the comfort of home, work, and public places. The online industry now offers an assortment of services, such as sports betting, casino games, bingo, lotteries, blackjack, and poker. Over 400 different companies in 48 jurisdictions provide online gambling at approximately 2100 registered sites, producing an estimated $20 billion in known revenues. Most of these jurisdictions are located in the Dutch Antilles, Malta, the Kahnawake Mohawk reserve in Canada, Gibraltar, the United Kingdom, and Australia (Williams & Wood, 2007, 2009). Possible precipitating factors for this expansion include easy access, convenience and comfort of online play, legalization and cultural approval, perceived financial value to consumers, widespread advertising, celebrity endorsements and corporate sponsorships, aversion to land-based gambling clienteles and environments, preference for player-to-player competition rather than fixed-odds wagering, and likeability of the structural characteristics of online games (Williams & Wood, 2009; Wood, Williams, & Lawton, 2007; Griffiths, Parke, Wood, & Parke, 2006).

At the same time, the spread of Internet gambling has raised several issues concerning problem gambling, consumer confidence, the fairness and integrity of the games, and the security of Web sites (Zangeneh, Griffiths, & Parke, 2008; McMullan & Perrier, 2007). In one study of online poker players, Wood & Griffiths (2008) found that cheating was a major concern for consumers. Players believed that *poker bots* operated by gambling sites were cheating them and that computer viruses were enabling some players to see other players' hands during play. In a second survey of Internet gamblers in 105 countries, Wood & Williams (2009) discovered that verifying the fairness of the games and identifying illegalities at gambling venues were major player concerns. Similarly, the American Gaming Association (2006) reported that about 50% of online casino players believed that Internet providers cheated them and 46% insisted that players cheated at play as well. Indeed, an international survey of over 10,000 Internet players found that about one third of them had had disputes with gambling providers and were dissatisfied with the complaint processes (Parke et al., 2007). McMullan & Rege (2007) discovered that gambling providers were also the victims of crimes such as cyberextortion, and Computer Emergency Response Team — Laboratoire d'Expertise en Sécurité Informatique (CERT-LEXSI) (2006), a French forensic firm, has reported that gambling companies were often the perpetrators and victims of international phishing schemes, identity theft scams, and money-laundering operations. Most recently, Giacopassi and Pitts (2009) have argued that Internet gambling is the latest victimless crime in the United States, and Ferentzy and Turner (2009) have outlined the many connections between gambling and organized crime. Rather surprisingly, however, there has been little in the way of a review or examination of online crime and Internet gambling even though it is an urgent research priority.

This study seeks to redress this absence by investigating the types, techniques, and organizational dynamics of virtual villainy at the portals of online gambling sites. It does not, however, examine the frequency of crime. We do not have reliable cybercrime statistics to calculate rates since "many cybercrimes go undetected and many detected cybercrimes go unreported" (Brenner 2007, p. 17). Our aim, therefore, is necessarily exploratory and qualitative in character. We ask the following questions: What types of cheats and crimes occur at online gambling sites? Who are the offenders? Who are the victims? How organized are cheating and cybercrime? Is there an organized-crime involvement in Internet gambling? How effective is legal governance in detecting, apprehending, and prosecuting cybercrime? Are conventional understandings of real-world gambling-related criminal behaviours and relationships altered by the digital environment of the Internet? Our purpose in writing this article, in part, was to stimulate debate and further research and help rectify a shortcoming that the research community acknowledges is pivotal but has so far failed to document and understand.

Method and approach

The World Wide Web is akin to a massive library. Yet despite the staggering volume of material, it has received only cursory attention from researchers interested in studying both criminal activity and gambling. Typical of the research to date have been studies of satellite hacking, telemarketing fraud, software piracy, sex crimes, pornography, stolen identity, cyberhomicide and cybersuicide, and the benefits and deficits of online gambling, including illegal business and player practices and gambling and organized crime (Mann & Sutton, 1998; McMillen & Grabosky, 1998; Shover, Coffey, & Hobbs, 2003; Taylor, Holland, & Quayle, 2001; Goodson, McCormick, & Evans, 2001; Jewkes, 2003, 2007; McMullan & Rege, 2007; Griffiths, Parke, Wood, & Parke, 2006; Griffiths & Parke, 2004; Schmalleger & Pittaro, 2009; Woods & Coats, 2008; Ferentzy and Turner, 2009; Williams & Wood, 2007, 2009). Research has tended to focus on readily available newsgroup sources and sites, player focus groups, interviews, and surveys and has ignored Web site features, chatrooms, blogs, and Internet interaction. We tried to be comprehensive in our approach and engaged a wide assortment of materials — video clips; media stories; online interviews; cheating kits and manuals; forensic, police, and security reports; and sociolegal documents — published between 2000 and 2008.

We used the Google search engine to retrieve our data. It coded more pages, created larger indices, and presented the most up-to-date data when compared to other search engines. We coded for 48 combinations of keywords, such as “cyberextortion and organized crime,” “player collusion and gambling,” “betting sites and fraud,” and so on. We sorted the data around four intersecting themes: online gambling; criminal techniques; the organization of cybercriminal practices; and legal control practices such as the efficacy of private cybersecurity, the quality of transborder policing, and the effectiveness of existing laws. The combination of keywords produced enormous quantities of page rankings, and we used a 10-page 100-article return process as a cut-off to obtain sample materials for each searched keyword. This criterion was a consistent means of retrieving data, and it ensured that each category was given equal weight and consideration. We retrieved 4800 documents, but the number of articles per keyword was repetitive after the first five or six pages. This in the end narrowed our materials to about 500 documents.

Because data about cybercrimes at gambling sites were not readily available from case law or field studies, we relied on document analysis as our research method. Document analysis may be defined as a way of analyzing texts in a systematic and qualitative manner for the purposes of exploring the classic questions of who said what, to whom, why, how, and with what effects (Mason, 2002; Maxfield & Babbie, 2001). While Internet documents were easy to access, use, and link and were sometimes presented in dynamic ways through threads, forums, and animations, there were some issues with quality control, accuracy of discovery, and consistency of documents over time. We dealt with these matters by relying primarily on authenticated Web sites such as news sites (e.g., MSNBC), security sites (e.g., McAfee), and law enforcement sites (e.g., FBI); by indexing every relevant article's uniform resource locator (URL) to create a registry of all document sources that could be checked and reexamined; and by triangulating multiple sources to verify information and look for missing data (Neuman, 2003).

There were, of course, many differences in the online crimes we studied. However, they all had one thing in common. They were acts where computers and information communication technologies were the agents, instruments, or targets of deviant or criminal events. We thus focused on the technical character of the illegal acts, the digital contexts that they occurred in, and the novel virtual socio-legal problems confronted therein. This approach stressed that at a given point in time certain illegal acts presented technical and social obstacles that had to be overcome for their successful completion, that we could identify and analyze the most efficient types of organization for managing these problems, and that the existence of different types of organization may be explained in terms of their technical efficiency in managing the online opportunities at hand (Best & Luckenbill, 1982; Grabosky, 2001; Brenner, 2002; Jewkes, 2003, 2007; Wall, 2007). Treating the rationality of an organizational entity as a potential explanation of its existence led us to ask the following questions: Was it possible for criminals working alone to plan and execute online cheats and crimes and manage the exigencies of online security? How did this nomadic form of cybercrime differ from the teams of digital *dot.cons* (i.e., Internet-based scams) that seemed able to develop collective attacks on diverse targets or from those even larger groupings that were able to establish enduring criminal networks?

Cybernomads

Toolkit cheats

We discovered that cybernomads were almost always solo criminal actors who stole or modified data, compromised computer systems, manipulated software for illegal purposes, or executed cyberattacks at online gambling sites. As one gambling consultant put it, “there are a number of groups trying to make money by hacking…. Where would you go? I’d go to dodgy online casinos” (cited in Warner, 2001, p. 2). Cybernomads varied with respect to their skills and motivations, but their strength was in their software and programming expertise and in their ability to exploit sites that offered businesses or players little protection (Penenberg, 1998; Keller, 1999; Kish, 1999; Zacharias, 2004; Brenner, 2002, p. 27). Toolkit cheats, for example, purchased prepackaged equipment such as scanners, sniffers, and snoopers; malware packages; password crackers; denial of service botnets; logic bombs; and algorithms that reduced their reliance on other organizational members to hack and crack gambling portals (Rogers, 2005; Gu, Liu, & Chu, 2004). Smoke Poker, for example, was an artificial intelligence program that gave cheaters the upper hand over honest players and providers in poker tournaments (International Game Developers Association, 2004). It was advertised as follows:

> 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. (SmokePoker.com, 2008, p. 2)

It included a sophisticated decision engine; advanced neural network technology; and an opponent-modelling system that monitored the poker tables, memorized opponents' game styles and betting patterns, calculated the pot and hand odds of winning, and then played the cards "in the best possible way, on auto-pilot!" (Brunker, 2004, p. 2; SmokePoker.com, 2008, p. 3; Yan & Randell, 2005, p. 3). One satisfied user 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%" (cited at SmokePoker.com, 2008, p. 1). Consider as well the HoldemGenius toolkit, which compiled advanced mathematical algorithms and allowed cheats to see their pot-drawing-out odds and odds of winning at over 100 online poker rooms, including PokerStars, Full Tilt Poker, BoDog, Party Poker, Titan Poker, and Absolute Poker. The algorithms were available from a fully functional Web site that also offered tutorials, customer support, and regular software upgrades to cybernomads. The latest update reviewed at the end of 2008 offered "bug fixes" at Party Poker, Full Tilt Poker, and Absolute Poker sites; "auto-resizing" at Titan Poker and Carbon Poker; and "upgrade support" at two- and nine-player games at BoDog.com (HoldemGenius, 2008b, pp. 2–3). Win HoldEm, another toolkit, promoted a "team edition" that allowed players to see one another's cards, in violation of rules against collusion. According to a company spokesperson, poker bots increased corporate profits by "35 percent in a five-day test in January [2004] in which it was used to play 7,000 hands" (cited in Brunker, 2004, p. 4).

Hackers

Other cybernomads were more advanced hackers. They manufactured malware, technical intelligence, and personal information or merchandised it to others via the underground economy. For example, one hacker offered computer spyware for $800, guaranteed it for six months, and accompanied it with a package of support upgrades (Jellenc & Zenz, 2007; Brothersoft.com, 2008, p. 1). Others created bot-networks using malicious codes that were covertly installed on personal or industry computers (McAfee, 2005; Symantec, 2007). These “zombies” were then activated for simple forms of intrusive trespass or herded into armies for more adventurous criminal projects such as cyberextortion (Skoudis, 2007; Morgan, 2005; McMullan & Rege, 2007). Botnet battalions were sold at various prices; 10 bots for a 24-hour “test-drive” sold for $5 US, small-scale attacks went for about $40 US, and 500 bots for one month cost $220 US (Biever, 2004, p. 1; Jellenc & Zenz, 2007, p. 43; McAfee, 2005, p. 13; O’Brien, 2000; Payton, 2005). Shadowcrew.com, CardersMarket.com, and CarderPlanet.com were the “Walmarts” of the cyberunderground, where digital loot such as credit card numbers and social security data were bought and sold in bulk packages and where cybernomads schooled each other on how to upgrade malicious activities for online gambling attacks (Arkin et al., 1999; Acohido, Swartz, & Ward, 2006, p. 1; McAfee, 2007, p. 10; McMillen & Grabosky, 1998; Payton, 2005; Symantec, 2007, p. 12).

Finally, cybernomads with the highest degree of technical acumen were akin to professional criminals. They executed prolonged attacks on their own and were more likely to have subcontracted their services to larger crime networks on a project-by-project basis (Rogers, 2005). One hacker, for example, targeted nine different sites for eight days, eventually closing down FullTiltPoker for 48 hours and disrupting Titan Poker so that it only loaded for a few hours on several of the eight days (Adair, 2008; Online-Casinos.com, 2008, p. 1; Jellenc & Zenz, 2007). Others lived off the data flow between gambling sites and players. They stole financial information from providers and conducted clandestine transactions in the customers’ names by assuming their legal identities. Other hackers were able to play both ends against the middle. They intercepted $100 wagers, credited $90 to their own accounts, and sent the remaining $10 to site operators. Then they intercepted the returning transmissions from the site operators. If the customer won, the hackers credited the customer's “phantom” account with $100. If the player lost, neither the player nor the operator realized that $90 had been diverted. The gambler assumed he or she lost $100, while the operator assumed the gambler lost $10 (Cabot, 2001). Still others, like Josh “JJProdigy” Field, used several accounts concurrently to cheat gambling providers and players. He won a $500,000 tournament but then deliberately lost the next tournament worth $140,000 to another player named ABlackCar. Party Poker discovered that JJProdigy had operated both accounts, cheating them and their customers of nearly $200,000 (Angerman, 2008). JJProdigy described his modus operandi as follows: “Sites can detect two things: IP [computer] addresses and the computer used. As long as you have different IP addresses and different computers, it is an easy stunt to pull off. For the different IP addresses, I simply used Verizon Wireless cards” (Ulick, 2007).

Characteristics of cybernomads

Cybernomads tended to operate alone partly because of the physical distance separating them online and partly because they competed with each other for digital loot. While they networked with people in digital stores and Web sites in order to obtain supplies, gain knowledge, plan strategies, and perfect attacks, they seem to have seldom needed partners or to have come into much contact with their victims. They emerged safely from online encounters by making use of superior technical force, secrecy impersonation, and quick attacks. They lived in the digital shadows and were prepared to take flight if necessary to evade industry, avoid victims, and escape legal agents with whom they seldom developed any stable *modus vivendi.* Cybernomads lived ubiquitous online lives and constantly shifted from one Internet venue or adventure to another. They combined skill with bravado to cheat and steal and to frustrate detection and capture. They often exaggerated their own qualities, especially when they were attacking or avenging gambling providers, which they often thought were beneath them. There was no leader-gang relationship among cybernomads, although they sometimes consulted with others or occasionally engaged in subcontracting practices. They shared a subculture but they did not usually hack with others. Digital loot did not have to be shared because the profits were almost always consumed by the principal actors or fixed at set commissions for services when merchandising arrangements were in force.

Dot.cons

Outside colluders

Cybercriminals also worked in dot.con teams that united for criminal projects that could be both occasional and ongoing. Players teamed up with other players, consultants, or Web site owners or managers to commit fraud, theft, and money laundering (Smed, Knuutila, & Hakonen, 2006; Yan, 2003). Most notable was the case at FullTiltPoker.com, where Chris “BluffMagCV” Vaughn was denied the $1 million prize he thought he had won at poker because he engaged in “seat-stealing”: selling his seat deep in the tournament to a more experienced associate, Sorel “Imper1um” Mizzi, for a percentage of Mizzi's prize. As Vaughn put it, “we were on instant messenger and I sent him [Mizzi] a message and it pretty quickly led to a discussion about selling the account” (cited in World Poker Rules, 2007, p. 1). Mizzi then logged on to Vaughn's account from home, and other players “faced a completely different BluffMagCV competitor, one with a different playing style and an incredible amount of online MTT [multiple-table tournament–Ed.] experience,” that opponents did not recognize and could not beat (Angerman, 2008, p. 2). While the gambling provider eventually tracked the account swap to Mizzi's home IP address, banned both players from the site, and deprived them of their potential winnings, one security expert noted that “if Sorel and Vaughn lived together, nobody would have known this happened.” He added, “this [seat stealing] isn't going to stop, because it's unenforceable" (cited in WPR, 2007, p. 1; Angerman, 2008). Indeed, Zie Justin and TheVoid are just two of the better-known cheating teams who played in large and small tournaments and surreptitiously deployed multiple accounts at the same cash game tables in order to purloin winnings from honest players (Woods & Coats, 2008; Moses, 2008).

Dot.cons also exploited gambling site data packets by inserting, deleting, or modifying game events or commands (Yan & Randell, 2005, p. 3; Yan, 2003, p. 3). The CheckRaised Rakeback calculator application that players placed on their computers to help track commission fees taken by gambling operators was a case in point. When the program was run it silently installed "Backdoor.Win32.Small.la" and other malware. This concealed the registry launch point from users, initiated keylogger scripts that retrieved users' login details, and spied on consumer interface connections to other poker applications. Customers' usernames, passwords, and account information were exposed and sent back to teams of hackers, which used the information for blackmail and identity fraud (Naraine, 2006; Sturgeon, 2005; Turkulainen, 2006).

Criminal insiders

Dot.con teams sometimes included gambling insiders, who provided and/or used privileged information for illegal purposes (Smed et al., 2006). The Absolute and Ultimate Bet scandals involving Tokwiro Enterprises and the Kahnawake Gaming Commission were exemplary. Suspecting unfair play, a player at Absolute Poker requested a history of the cards he was dealt during a high-stakes poker tournament. He received a detailed log of every player's hand history and IP address by mistake and discovered that at each table at which "Potripper" played, another account, "#363," was a "spectator." Indeed, once #363 entered the tournament, Potripper 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). Investigations eventually linked #363's IP address to an employee of the company and the Potripper account to a former executive of the company. According to the Gaming Commission, the perpetrator was a "high ranking trusted consultant with access to its security systems" (Kahnawake Gaming Commission (KGC), 2008a, p. 2). The insider consultant had real-time access to all the hole cards on all the hands and had relayed this information to his associate, Potripper. Between them, Potripper and #363 stole between $500,000 and $1 million from players over at least six weeks of undetected illegal play (Goldman, 2007; Levitt, 2007). In addition, six other "superuser accounts" — GrayCat, PayUp, SteamRoller, XXCashMoneyXX, DoubleDrag, and RonFaldoXXB — discarded "hands on flops despite raising preflop," suggesting that they too were aware of their opponents' hole cards and were part of a larger web of account deception and inside corporate collusion that was taking money from consumers without much fear of detection or prosecution from either the company or the regulator (Casinomeister, 2007, p. 7; KGC, 2008a; Moses, 2008).

In the case of Ultimate Bet, two players, “Tramboplaine” and “dipnyc21,” reviewed their hand histories in several tournaments and found that one account, “NioNio,” had won 13 of the 14 sessions and banked $300,000 in profit in just 3000 hands. This win rate was 10 standard deviations above the mean, or “approximately equal to winning a one million dollar lottery on six consecutive occasions” (Moses, 2008, p. 2). NioNio, in fact, was at the centre of several dot.con teams that changed usernames repeatedly to cheat players and evade detection (KGC, 2009, p. 6). Eventually it was discovered that NioNio had obtained an unfair advantage through “unauthorized software code that allowed the perpetrators to obtain hole card information during live play” (KGC, 2008b, p. 2). The code was written by individuals who worked for Excapsa Software, which had a corporate relationship with E World Holdings, a previous partner of Ultimate Bet, which then used the software to cheat the new owner (Tokwiro Enterprises) and thousands of customers of about $22 million. A total of 23 “super user accounts” involving 117 virtual personas were deployed by 31 industry insiders and associates to cheat consumers over 55 months of play from June 2003 to December 2007. The vast majority of the computer devices, IP addresses, and player accounts used to cheat and transfer money had ties to the E World Holdings Group and/or Russell Hamilton, a former world series of poker champion. Excapsa, which sold the faulty software to Blast Off Ltd., a company controlled by Tokwiro Enterprises, has paid out a $15 million lawsuit settlement that has been used to compensate some players for the losses that occurred before and during Tokwiro's ownership of Ultimate Bet (KGC, 2009; Hintze, 2008; KGC, 2008b; Swoboda, 2008; Polson, 2008).

Not only were corporate insiders involved in fraud, some engaged in theft by withholding winning revenues or by creating phantom sites and malware to steal from potential customers (Andrle, 2006; CERT-LEXSI, 2006; Games and Casino, 2006; Kvarnstrom, Lundin, & Jonsson, 2000; Zacharias, 2004). Several gambling sites, for example, were set up as fly-by-night businesses. Site operators simply transferred potential customers’ funds from their business accounts to their personal accounts and then disappeared into the ether of the Internet (Cabot, 2001; CERT-LEXSI, 2006; Heinrichs, 2001; Penenberg, 1998; Zacharias, 2004). Others designed fake Web sites with fancy graphics, fraudulent licences, and phoney company phone numbers and e-mail addresses and stole consumers’ identity data under false pretences. Still others, such as GlobalSportsNet, defrauded customers by not mailing them their winnings, while others, such as “Fallons” and “Bingo World,” shorted their customers on their returns (Arthur, 1997, p. 1; Kelley, 1997; Shaw, 2004). As Finch (2007) rightly observes, “the key value of the Internet in connection with identity theft and fraud is the way in which it shields the true identity of the fraudster from those with whom they interact online” (p. 10).

Employees of gambling sites also teamed up with dot.con teams in crimes against their employers (Rogers, 2005). Employees, for example, sold company secrets, including account information, gaming software, and sophisticated algorithmic programs for deciphering random number generators, to hackers who then cracked into gaming servers, altered their programs, and ensured that “every roll of the dice in craps turned up doubles, and every spin on the slots generated a perfect match; … cherries across the board” (cited in Reuters, 2001, p. 1; Warner, 2001; McMullan & Perrier, 2003, 2007). Perhaps the best-known reported case of employee-generated crime involved Starnet Communications, where highly placed employees cheated its licensees of 85% of net sales. Employees created “fake” winner accounts with modified betting histories. They changed a $20 win for a $20,000 win and deprived the licensee of $19,980. Starnet's accounting unit then paid the supposed winners out and tampered with company records to cover up their workplace crime (Gambling Magazine, 1999).

Botnet herders and small-scale organized crime

Digital teams sometimes used bots to launder money through gambling sites. One team, for example, swamped poker rooms with inferior poker bots. Dot.con members then played against and defeated the weaker staged bots, allowing money to change hands, with team members dividing the take and cleaning the capital before botnet hunters could find them (OnlinePoker-News.com, 2007). In other instances, botnet battalions programmed to wager, pick cards, and fold were used to flood casino gaming rooms with illegal capital. Bot-herders took the last seats in the games, easily beat the zombie armies they had mustered, and cashed out the winnings as “clean” money from the casino or poker room accounts (Sullivan 2007). As one security officer observed, “phishers set up online gambling accounts using stolen credit card numbers and victim's identities … and launder dirty money by exchanging funds through the pots of games they set up amongst themselves” (Leyden, 2008, p. 1). Still other dot.con teams engaged in “chip dumping”. Proceeds from crime were deposited into fake customer accounts and deliberately “lost” to associates at gaming tables who then cashed the dumped winnings into a network of accounts, further smoothing the cybertrail from criminality to legality (RSe Consulting, 2006). Finally, some teams used offshore gambling sites to launder funds. From 1998 to 2005, for example, www.BetWWTS.com illegally enticed US gamblers to place wagers on sports events. The owners sequestered the bets, moved their illegal capital to shell corporations, and transferred the money to clandestine accounts in foreign banks in the Caribbean (Ames, 2006; Department of Justice (DOJ), 2006).

Lotteries were also associated with fraud involving teams of dot.cons, and

MaxLotto was a case in point. Licensed in the Dominican Republic in 2001, it advertised that 10% of its worldwide $100 million lottery revenues would be donated to charities (Kelley, Todosichuk, & Azmier, 2001; PRNewsWire, 2001). By 2002, however, MaxLotto.com had disappeared from the net with its customers' capital. No prizes had been paid out and few of its listed benefactors knew of the company or had received donations from it (Bortz, 2008). Or consider the lottery fraud that occurred in India in 2007, organized by a three-handed team. The leader, Albaika, recruited Acharya online to serve as the broker for Sagwekar and other teams of agents he had commissioned to set up bogus bank accounts in Mumbai. Then Albaika sent a mass email across India congratulating many players on winning a lottery worth millions of rupees and instructed them to deposit funds for service charges into bank accounts as a condition of receiving their jackpots. Once the money was deposited, however, Albaika used his network of agents to usurp the clients' funds, estimated to be about $8 million (Times of India, 2008).

Characteristics of dot.cons

Dot.cons approached cybercrime as a working trade and developed established routines for taking money from a large number of victims. Three circumstances favoured the establishment of this form of illegal activity. First, the dramatic expansion of Internet gambling over the last decade meant that people from near and far carried large quantities of personal e-cash in online gambling accounts or in the form of large tournament prizes. Cheats travelled from one gambling site to another following sport-betting opportunities, card competitions, casino games, lotteries, and other events that attracted online crowds. Hackers fleeced novice operators as they set up their businesses on the net, and commercial insiders who designed software and administered gambling venues conned and stole from the virtual strangers and partners who passed through their Internet portals. Dot.cons thrived by targeting many consumers simultaneously, by not taking too much from any one victim at any one time, and by harvesting many online personas so that consumers did not know that they were cheated or defrauded until long afterward or not at all. In such circumstances attempts at player and property protection and security and law enforcement were not especially energetic or effective, either because the crimes were automatic and difficult to detect or because they were mostly minor in their personal and economic consequences and not likely to result in many formal complaints or legal actions. Second, in the digital world of multiple make-believe names and easily given trust, cybercheats, cybercons, and cyberthieves were fairly safe if they could evade detection and avoid confrontations with virtual victims while they were online. Once away from cyberspace they could melt into their own social worlds, assume their offline identities, live like other citizens, and return later to the Internet with new proxy identities (Finch, 2007). Finally, the scale and density of Internet gambling sites, activities, and users as well as other commercial venues meant that there were enough criminals on the net to form hacker undergrounds, within which techniques of crime could be developed, innovated, and passed on over time. As Cere (2007, p. 148) puts it, hacking has become the “veritable ethic” of the information age. It ranges from benign thrill-seekers to net-dedicated hackers to more criminally oriented digital teams and networks.

The result of these circumstances is that dot.con teams have been able to establish a *modus vivendi* with industry and law enforcement such that overt conflict has so far been minimal. Punishments to date have not been very severe, and detection and arrest seem to have followed only a small fraction of the crimes committed, as evidenced by comparing the outcomes of the Absolute and Ultimate Bet poker scandals. To date no offenders have been arrested or charged, and most have been protected from public exposure and granted *de facto* immunity from legal action by both gambling companies and regulators. The trick of the dot.con trade has been to reduce the likelihood that their crimes can be detected, reported, and acted upon so as to limit public tips and complaints and minimize police involvement. This has not been that difficult because crime control in virtualized worlds remains relatively underfunded, poorly resourced and organized, and especially difficult to apply in shifting, borderless contexts (Aas, 2007; Brenner, 2007; Jewkes & Andrews, 2007; McMullan & Rege, 2007). The typical form of organization for dot.con teams has been a flexible group consisting of two to six associates that participated in particular criminal events in which each person had specialized roles to play in the crimes that they conducted, such as programming attack tools, creating malware, herding bots, and manipulating player accounts. Unlike with cybernomads, however, there was an elementary leadership feature as well as a principle for dividing profits. The most common rule appeared to be that novices followed the lead of more experienced dot.cons and that payouts were negotiated in advance of jobs and mostly honoured once a criminal event was completed. As Holt (2009) observes of the hackers he studied, those who formed “teams” tended to be more sophisticated, lasted for longer periods of time on the Internet, and had a more developed stratification structure when compared to hackers who performed alone.

Assemblages

Cyberextortion rings

Crime assemblages constituted a third type of organization related to Internet gambling and are best exemplified by the cyberextortion attacks of online sites between 2000 and 2006. The distributed denial of service (DDoS) attack is the typical technique, and it usually began with bots that were herded into an army weeks or months before attacks were scheduled (Paulson & Weber, 2006; Ratliff, 2005; Golubev, 2005). Bots then swamped gambling providers with bogus requests that consumed all available disk space and CPU time, bandwidth capability, or physical network components and denied services to legitimate customers (McMullan & Rege, 2007; Paulson & Weber, 2006, Murphy, Pender, Reilly, & Connel, 2005). Once the sites were slowed or shut down, ransoms in return for protection from further attacks were demanded. “Dear wwts, as you can see your site is under attack. We have found a problem with your network,” stated one e-mail. The attackers then insisted that gambling sites wire cash ($40,000 to $50,000 US) to offshore bank accounts in multiple $10,000 packets: “You will lose more than $40,000 in the next couple of hours if you do not resolve this problem,” one attacker warned (cited in Karshmer, 2005, p. 1). If the operators did not pay up, the attacks continued and the sites suffered further disruptions and demands for tribute (Warner, 2001; Cassavoy, 2005; Germain, 2003, 2005).

Hundreds of gambling sites were subjected to DDoS attacks, and cyberextortionists inflicted over $70 million in reported overall damages to British bookmakers alone in 2004 (Nutall, 2004). Canbet Sports Bookmakers, for example, suffered a DDoS attack during the Breeders’ Cup that cost them more than £100,000 in revenue every day the site was shut down. In 2003, BetCris was warned 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” (as cited in Ratliff, 2005, p. 4). BetCris did not comply and it took the cyberextortionists less than 20 minutes to take down the site. In 2004, Multibet also refused to pay tribute. That site was attacked four times and the business was interrupted for 20 days until a reluctant CEO wired the protection money to an eastern European bank account (Jellenc & Zenz, 2007; McMullan & Rege, 2007).

Cyberextortion networks had an elementary division of labour that included organizers, extenders, and executors (Lemieux, 2003). Organizers arranged plans to be conducted by other subnetwork members. They often shifted from legitimate activities to exploit new online opportunities in the gambling field (Gray, 2005). The mastermind in one cyberextortion ring, for example, was a 21-year-old mechanical engineering student who studied computer programming before starting to hack gambling sites for a living (Computer Crime Research Center (CCRC), 2005; McConnell International LLC, 2000). Other organizers worked at the behest of international syndicates that provided the capital to finance attacks at online sites (Germain, 2004; Williams, 2002; Walker, 2004).

Extenders were mainly recruiters who screened new members and added to the skill sets of the networks. For example, one hacker was “contacted by a couple of different criminal organizations that offered him quite a bit of money,” and known associates of his had also been hired by “various organized crime groups” (cited in Public Broadcasting Service, 2001, p. 3). As one law enforcement agent observed, hackers know that if they are clever they can “use it to earn a living” with an international outfit (cited in ZDNet, 2005, p. 1). Executors were the front-line agents, who possessed practical knowledge of reverse engineering, virus installations, and architectural vulnerabilities. They banded together to implement DDoS attacks against gambling sites from around the world. For instance, one cyberextortion ring had members in Moscow, St. Petersburg, and Saratov who had never met face to face. As one police officer observed, this was “not a normal organization. Everyone sat at home, and everyone had their role” (cited in Bullough, 2004, p. 2). While subunits communicated with each other via organizers, the latter need not know other members. This separation of tasks and personnel resulted in a remote compartmentalization structure that guaranteed a fluid, flexible, and smooth-functioning network with regenerative characteristics. For example, three hacker rings running DDoS attacks against U.K. bookmakers also made 54 similar attacks in 30 other countries for six months worth an estimated $4 million U.S. (Leyden, 2006). So these mafias of the minute have required fewer interpersonal contacts, fewer relationships based on sponsorship and discipline, and fewer hierarchical command systems to commit crimes when compared to conventional real-world organized-crime groups (Brenner, 2002; Council of Europe, 2004; McAfee, 2005; CCRC, 2005; Gray, 2005; Ferentzy & Turner, 2009).

Phishers and identity fraud

Cyberassemblages also used gambling sites to conduct identity scams, but on a grander scale than dot.cons. One criminal network, with the help of an insider, hacked into BetOnSports’ database and stole account names, addresses, phone numbers, social security numbers, and credit card and bank account numbers, which they then used for illegal purchases and identity fraud all around the world (DOJ, 2007a; Mark, 2007; Costigan, 2007; United States Attorney Southern District of New York (USASDNY), 2008; Caray, 2006). Another cyberassemblage combined confidence cheating with identity theft and deployed the real addresses of the lottery Euromillion Espana to swindle consumers of over $200 million in France, Australia, Netherlands, Britain, Romania, and East Africa (elGordo.com, 2008, p. 1). Some network members were akin to forgers and created fake sites and administrative documents. Others, specializing in social engineering, posed as representatives of elGordo.com and sent convincing emails to consumers. They obtained confidential customer information through three phishing techniques: (i) the deceptive attack, where users were tricked by fraudulent messages into releasing their information through the lottery to crime groups; (ii) the malware attack, where malicious code placed on customers’ computers retrieved confidential user information without their consent; and (iii) the Domain Name System (DNS) attack, where the IP addresses of lottery sites were altered to send victims to fraudulent servers (Emigh, 2005; CERT-LEXSI, 2006; Barrett, 2004).

While Spanish police eventually arrested some members, the crime network continued to function despite international police investigations and court prosecutions (Queen, 2007, p. 1). A third example involved PartyPoker.com, where phishers working in an elaborate criminal enterprise designed a perfect replica of the gambling site and hosted it on their own illegal servers. PartyPoker's customers were sent e-mails warning of US legislation that would affect them and were told to take remedial action by clicking a link to the cloned site's login page. Those who complied were directed to a phantom venue, where they were prompted for personal information that was then used to (i) sell legal identities for criminal use, (ii) simulate real user accounts so that network members could impersonate players and gamble in their place, (iii) steal playing credits from online gambling accounts, and (iv) merchandise digital data to competing gambling sites (Chen et al., 2005; Emigh, 2005; Thompson, 2007).

Money-laundering enterprises

Criminal assemblages also operated or worked in tandem with Internet gambling sites to further other criminal pursuits. From 1997 to 2008, for example, US state and federal courts have charged and convicted gambling companies such as World Sports Exchange, World Interactive Gaming Corporation, Golden Chips Casino, Paradise Casino, Gold Medal Casino, Betcris, Dukesports, Betcorp, Betwwwts, BetonSports, Bettheduck, Sportingbet, and Safedepositsports for crimes including conspiring to violate the Wire Wager Act, tax fraud, illegal gambling, money laundering, racketeering, and enterprise corruption. While many of these prosecutions were for engaging in or enabling illegal sports betting using phone lines and computers on the Internet, several had complex structures involving formal organized-crime elements.

The Giordano money-laundering enterprise is a good case in point. Members of this network were adept at moving unlawfully earned proceeds through online casinos, shell corporations, and bank accounts to Central America, the Caribbean, Switzerland, and Hong Kong. The executors involved front companies that developed the gambling Web site www.playwithal.com, which enabled approximately 40,000 customers to set up accounts and place bets on football, baseball, golf, and other sports events. Giordano, the organizer, ran the strategic operation of the network; his son-in-law, the controller, oversaw the everyday operations, managed bettor information, and handled Internet accounting matters and discrepancies; and his wife and daughter, the financial officers, laundered crime proceeds to several offshore banks. Five other individuals acted as street-level clerks, runners, and enforcers, collecting bets; distributing, delivering, and transferring illegal gambling proceeds between members; and maintaining network and bettor discipline when necessary (CERT-LEXSI, 2006; North Country Gazette, 2006; Venezia, Martinez, & Livingston, 2006).

The Uvari Bookmaking network also combined an illegal gambling business with money laundering and tax evasion. They had network members and clients in New York, New Jersey, Florida, Nevada, North Dakota, New Hampshire, and Oklahoma, as well as in offshore locations, such as the Euro Off-Track in the Isle of Man and the Elite Turf Club in Curacao. The Uvari Group operated as an intermediary between gamblers and sport-betting companies. They determined their "take" based on the volume of accounts they opened at offshore sites and always returned a portion of their commissions to bettors as an incentive for them to continue using their bookmaking facilities. They created customer accounts for individual bettors, took their customers' personal information, and attached it to the social security numbers of group members, creating hundreds of dummy accounts in their own names. This permitted customers to remain anonymous and avoid paying taxes on winnings and, simultaneously, allowed the Uvari Group to launder money and claim income tax deductions by associating their customers' losses with their own accounts (CERT-LEXSI, 2006; USASDNY, 2005, pp. 1–6; DOJ, 2007b, pp. 1–6).

Finally, the Corozzo network engaged in an illegal gambling and loan-sharking enterprise that was based in the United States and Costa Rica. The network of at least 26 members relied on toll-free telephone numbers and four online betting Web sites to handle thousands of sport wagers each month from November 2005 to January 2008, amounting to an estimated take of $10 million. A controller ran the operations, resolved bettor and accounting disputes, and managed account information, and three agents oversaw the offshore accounts, calibrated wins and losses, counted the weekly take, and advised the controller regarding economic matters. In addition, an onshore clerk accepted wagers over the telephone and recorded them on audiotape and on paper, six money collectors transferred gambling proceeds between members of the organization and financial institutions, and 13 runners managed bettors by accepting wagers and setting up login codes and passwords. Finally, two enforcers lent money at exorbitant interest rates to troubled bettors and instilled fear in all bettors not to miss their payments (District Attorney Queens County, 2008, pp. 1–5; North Country Gazette, 2008, pp. 1–3; Ginsberg, 2009).

These case studies suggest that Internet gambling sites are ideal for money laundering and other complex fraudulent and extortionist activities that, in turn, can finance yet other crimes. Despite the strict codes for reporting financial transactions, money launderers seem able to function by manipulating accounts, making smaller cash exchanges, putting players "on the take" on their payrolls, hiding transactions in a bewildering array of gambling and bank accounts, and mobilizing fear when necessary.

Characteristics of criminal assemblages

Criminal assemblages were structured as ongoing projects or businesses rather than as crafts or solo operations. Unlike the “short cons” of the dot.con teams, which were often intermittent events, the “big cons” of the criminal assemblages relied upon the time-honoured methods of long firm fraud: the willingness of a large number of victims to supply credit and information and to invest or agree to acquiesce to schemes that promised to pay well over the odds. This culminated in the establishment of clever illegal business premises on the net where victims were relieved of both identity and capital before bankruptcies were declared or corporations disappeared. This was especially apparent with the *modus operandi* of cyberextortion groups whose organizations were remotely controlled rather than directly and locally managed. Nodal subnetworks in extortion rings coexisted in a dispersed lateral field of global information flow. The virtual rings that brought down gambling sites were dynamic, international pods of loosely connected groups. The networks supplied contact points to assemble criminal endeavours and to develop counteractions against reluctant or resistant victims, competitors, or law enforcement agencies, after which they usually dispersed, only to resurface later (Brenner, 2002; McMullan & Rege, 2007).

However, because larger amounts of money were being appropriated in an increasingly visible way, gambling providers, regulators, police, and private security companies necessarily stepped up their efforts to prevent it. Criminal networks and public and private law enforcement agencies were more and more engaged in techno-wars, which had a tendency to escalate as each side improved their techniques to outwit and outflank the other. One consequence was that assemblages had to be prepared to take greater chances, including raising the risks involved in marketing their products and using direct confrontations with their victims while simultaneously upgrading their techniques and planning to minimize these higher risks. The danger of recognition in victim confrontations at virtual venues was reduced by upgrading the speed of operations and by deploying ingenious aliases, clones, and simulations. The danger that information might be leaked before or after the commission of crimes was reduced by remote planning, careful recruiting of members, secret meetings, and prudent online behaviour that aroused as little suspicion as possible. The danger of exposure was reduced by communicating via screen identities that were difficult to trace and by engineering trust in the act of crime. In short, speed, anonymity, synchronization, and coordination were arranged as much as possible in advance so that criminal acts appeared as “natural” as possible and aroused few suspicions.

A second consequence was that operations on this scale become known to corporate and government agencies, and their success depended on the ability of the industry and the state to suppress them. Certainly victims — *bona fide* lotteries, online betting shops, and Internet poker rooms — took more precautionary licensing and registration measures, developed better internal security measures, hired private cybersecurity firms, and tried to mobilize existing law enforcement agencies to help them combat criminal networks. Without a doubt, US authorities have cracked down on the sport-betting market and its software and payment-processing companies in an effort to restrict the reach of Internet gambling Web sites (Geiss, Brown, & Pontell, 2009). However, cybercrimes of an international sort are especially difficult to discover and limit by traditional law enforcement bodies, third-party multilateral policing partnerships, and victims using self-help market-based solutions. The laws governing cybercrimes occurring at Internet gambling sites were and remain imprecise and confounding as to where offences occurred (i.e., whether in the country where criminal networks were based or in the jurisdiction where the crimes happened), where evidence should be collected, what laws applied and in what jurisdiction, what courts prevailed, and what sanctions were appropriate.

This ambiguity surrounding legal guardianship was compounded by the fissured structure of law enforcement within and between nation-states, making the policing of cyberassemblages complicated, costly, and occasional. Many police forces simply did not have the reach, resources, or expertise to investigate crimes that were committed from remote places in multiple sovereign jurisdictions where the offenders were not even present. As the deputy director of SRI International put it, the botnet-hunting community “is two or three years behind in terms of response mechanisms” (cited in Naraine, 2006, p. 2). Cybercrimes committed from across the globe have played ducks and drakes with international law enforcement agencies, which lack enforceable international instruments, effective transborder crime management measures, and up-to-date forensic tools, resulting in low public visibility of gambling-related crimes, few successful prosecutions, and for the most part, paltry penalties (Nhan & Huey, 2008; Moore, 2007; McMullan & Rege, 2007; Jewkes & Andrews, 2007; Smith & Wynne, 1999).

The weakness of global legal governance has encouraged multilateral policing by private-sector providers and digital security firms and fostered self-help business solutions reliant upon authentication and encryption technologies. This has meant investing in business opportunity reduction remedies such as detection systems, enhanced firewall protection, and patch and configuration systems to limit malware infections and software compromises, and in intelligent web-based products such as parallel network intrusion prevention architectures and self-correcting software to identify, filter, and divert illegitimate traffic from gambling sites to improve security. But these reforms have not eliminated the problems. To start, the relations between private and public agencies have not always been workable. The case of Don Best Sports, which was extorted for $200,000, is illustrative of this problem. A computer security company tracked the cyberattacks to a chat room in Kazakhstan, but when they notified the FBI and the Secret Service, the latter “threw up their arms because it was in Kazakhstan,” said the CEO of the private security company (cited in Ratliff, 2005, p. 3). Furthermore, resorting to multilateral policing and self-help solutions has been costly. Many gambling companies cannot afford the expensive investments in hardware, software, maintenance, and upgrading. The result is a global patchwork of private self-help fiefdoms that afforded security to some but created few industry-wide standards on safety and protection and little consensus about the best devices to stop cybercrimes early and at a distance from gambling venues. Finally, authentication and encryption technologies have created an underground cottage industry in devices and schemes to circumvent these security tools. As cybersecurity has evolved, the high-level plans of cyberthieves, cybercons, and cyberextortionists have disguised attacks, intrusions, and simulations at their point of ingress into gambling site networks; tested the guards, tech boxes, switches, and detectors for anomalies and weaknesses; and probed the new multilateral and commercial security systems for gaps, lapses, and intelligence. A never-ending cycle of enhanced detection and counterdetection measures has proliferated to rationally handle the technical problems of crime and negotiate the exigencies of legal control on the Internet, resulting in an online marketplace that remains replete with criminal potential (Jewkes, 2007; Nhan & Huey, 2008; McMullan & Rege, 2007).

In sum, crime assemblages were more formal and continuous in operation when compared to the two other kinds of online criminal organization. They were more sophisticated than dot.cons or cybernomads, had the most elaborate division of labour for engaging in criminal behaviour, and lasted for an extended duration across time and space. However, despite the more complex stratification system and apparent ability to neutralize formal law enforcement, there is no evidence that these crime networks coordinated their activities into cartels, purchased immunity from the state by bribery or influence peddling, or imposed a monopoly either by consent or coercion over cybernomads or dot.cons. There is no tendency toward a business enterprise type of organization where the former usurps or administers the latter. If anything the economy of online gambling-related crime is in a state of vertical malintegration. So there appears to be no managerial rationality, where one entity is capable of running other online crime groups. More likely there will be no sudden disappearance of cybernomads, dot.cons, or crime assemblages from Internet gambling sites in the near future.

Cybercrime, real-world crime, and online gambling

Not all deviant or criminal activities occurred solely in cyberspace or solely in physical space, and these raise the relationship between offline and online realms in criminal relations and Internet gambling. To date, online aspects of crime and terrestrial counterparts tend to be studied as separate realms. Real-world crime is seen as (a) physically proximate, (b) one-to-one in scale, (c) limited by geographically and demographically demarcated areas and their risks, (d) patterned into predictable trends and rates, and (e) policed by law enforcement agencies that can concentrate their resources where they think these crimes are most likely to happen. Online crime is seen as (a) not constrained by physical proximity between victim and offender for the consummation of an offence; (b) automated so that an offender can commit thousands of crimes quickly, affecting many victims simultaneously; (c) located in electronic environments where information flow dematerializes space, crime scenes, physical evidence, and criminal identity so that it is difficult to determine where a crime occurs, uncover evidence about it, and identify credible suspects; (d) not recorded in discrete categories or patterned into reliable statistics; and (e) not easily policed by law enforcement agencies, which cannot easily identify offender-offence-victim patterns to deploy their resources to deal effectively with criminal events (Brenner, 2007; McMullan & Rege, 2007; Jewkes, 2003; Grabosky, 2001).

While these differences are no doubt important, our investigation suggests that there are also many contact points where the virtualization of the Internet is inscribed into real-life events and contexts and vice versa, resulting in the intermingling of online and offline worlds and the development of new hybrids around crime and Internet gambling (Brown, 2006). The first lesson from this study concerns the *space of crime*; cheating and cybercrimes at gambling sites were increasingly planned and executed in *hybrid space*, and neither cyberspace nor physical space was predominant in criminal conduct. Thus territory and distance were different from those conceptualized solely in cyberspace or solely in physical space. Hybrid territory at Internet gambling portals was both finite and infinite, sites were both remote and proximate, and distance existed and disappeared. Cybernomads, dot.cons, and cyberextortionists committed crimes by “jacking into” cyberspace and then disconnecting to return to physical space. They did not leave either world behind in the consummation of their crimes but rather followed a process of weaving online communications, identities, and activities into their existing offline lives and vice versa, for purposes of criminal behaviour.

The second hybrid concerns criminal identity when actors, teams, and networks blur the boundaries between real-life experiences and personas and virtual experiences and screen identities. The terms “criminals” and “cybercriminals” as *sui generis* categories emphasize the boundaries between the embodied real and the virtual and fail to appreciate the ways in which the virtual is inscribed into the real world of crime and vice versa, creating *hybriminals*, who experienced and interacted in an infinite space when they attacked gambling sites remotely through anonymous, combinatory, and repetitive techniques and then returned to physical zones where interaction, distance, and space were finite. This flow of space and blending of worlds (finite/infinite, remote/proximate) increased the *scope* of criminal organizations at gambling sites. So while sites of victimization were located in cyberspace (poker rooms, casinos, lotteries), sites of planning, coordination, and implementation occurred in several physical and digital territories simultaneously. Hybriminals met face-to-face in physical space and then logged into cyberspace under countless identities to attack customers and providers all over the world. Alternatively, they consummated crimes online using stolen or fabricated identities and, fearing exposure, retreated into physical zones to avoid, evade, or neutralize detection. This ability to move, turn, and return gave hybriminals substantial control over their criminal techniques and movements; expanded the nature of criminal agency and the scope of criminal events; limited the potential for detection, apprehension, and arrest; and kept crime organizations relatively anonymous, flexible, and regenerative.

The third hybrid concerns the blending of the virtual and the physical and how it impacts the speed of criminal events, resulting in a new notion of time for crime. On the one hand, real-world elements of criminal events at gambling sites certainly entailed planning and execution that extended over linear time-frames (e.g., bookmaking schemes, money laundering). On the other hand, online elements tended to form and dissolve almost in an instant, only to reappear in circular repetitive cycles of time (e.g., hacking, DDoS attacks, digital ransoms). So hybriminals crossed over and engaged with various notions of time and combined the fast-forwarding of virtual spaces with the slow-motioning of terrestrial spaces to consummate crimes at gambling sites continuously/intermittently, concurrently/chronologically, in real time/in chosen time, and for short/long durations. They operated at the portals of Internet gambling in *hybrid time* according to a series of information breaks and flows where offenders could literally “time” their crimes, record and repeat them, delay and divert them, or even cancel them while they were occurring. Thus crimes at online gambling sites combined recursive and linear time elements that afforded perpetrators even greater control over the planning of their criminal activities and the speed of their execution (Bogard, 1996; Brown, 2006; Wall, 2007).

The fourth form of hybrid concerns the character of assemblages. Crime networks operating primarily in cyberspace (e.g., cyberextortion rings) tended to be lateral in structure, with fleeting memberships and weakly developed horizontal divisions of authority, while those more rooted in real-world environments (e.g., bookmaking schemes) tended to be stable formal organizations with vertical authority structures. *Hybrid assemblages*, however, exhibited the characteristics of both land-based and digital criminal organizations. They recruited confederates in both physical and digital spaces. Technological skills were discovered and deployed in online environments, while skills such as meeting with partners and picking up ransoms were used in physical space. Hybriminal assemblages had access to a wider set of criminal expertise, which when directed at gambling targets fashioned new alliances between hackers and organized-crime groups and unconventional divisions of labour involving the subcontracting of specialist services. Hybrid assemblages were a mix of old and new features, combining digital techniques such as DDoS attacks, virus and malware manipulations, and phishing with traditional techniques such as confidence cheating, embezzlement, and forgery.

The final hybrid form concerns governance in the borderless world of online gambling. Effectively governing crime in fluid contexts requires a more flexible form of techno-policing that can function in the spaces of connectivity between the virtual and the real. Defensible Internet spaces now necessitate inventive online architectural solutions and better offline law enforcement, but they especially require more proactive digital security networks that are responsive to both virtual attacks and real-world harms. Forward-looking systems of crime control will need to mobilize and integrate political nodes, law enforcement nodes, industry nodes, and citizen nodes into a comprehensive system capable of pooling technical resources, expert knowledge, and trained personnel to form new security regimes for gambling habitats. This means that online players will have to take greater responsibility for the security of their computers to limit hacking and botnet herding. Suppliers of devices, software, hardware, and critical infrastructure will have to be more accountable in law for ensuring that the technologies gambling consumers are provided with on the Internet are reliable and can prevent cheating and fraud. Law enforcement agencies will have to be organized to participate fully in multilateral policing that increases the internodal bandwidth for discovery and detection of wrongdoing and strengthens the density of nodal relationships in the security of online gambling environments to divert and repel cyberattacks, identify identity fraud, and restrict money laundering (Johnston & Shearing, 2003; Williams, 2006; Wall & Williams, 2007).

In sum, users, providers, and architects of online gambling sites have good reason to express concern about the protection of private information, the integrity of the games, and the security of Web sites because Internet gambling has been a source of crime, a vehicle for crime, and a support for crime. Like other forms of Internet commerce, it has not been immune to criminal exploitation, and like other forms of Internet commerce, what is beyond doubt is that the cases that come to the attention of the industry, regulatory authorities, consumers, and academic researchers are likely to represent the tip of the iceberg.

References

Aas, K.F.. (2007). Beyond “the desert of the real.” Crime control in virtualized reality. In Jewkes, Y.. (Ed.), *Crime online*. Cullompton: Willan.

Acohido, B.. Swartz, J.. Ward, S.. (2006, October 12). Cybercrime flourishes in online hacker forums. *USA Today*. Retrieved November 14, 2006, from http://theadvertiser.gns.gannettonline.com/apps/pbcs.dll/article?AID=/20061012/TECH01/609070348/1001/tech.

Adair, S.. (2008, February 18). *Gambling websites under attack*. Retrieved November 28, 2009, from http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080218.

American Gaming Association. (2006). *Gambling and the Internet: The A.G.A. Survey of Casino Entertainment.*Washington, DC: American Gaming Association.

Ames, B.. (2006, May 18). Internet gambling operators indicted. *PC World*. Retrieved April 2, 2008, from 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?*PokerPages*. Retrieved March 23, 2008, from http://www.pokerpages.com/articles/archives/angerman03.htm.

Arkin, B.. Hill, F.. Marks, S.. Schmid, M.. Walls, T.J.. McGraw, G.. (1999, September 28). How we learned to cheat in online poker: A study in software security. *Developer.com.* Retrieved November 28, 2009, from http://www.cigital.com/papers/download/developer_gambling.pdf.

Arthur, C.. (1997, December 7). Suckers pour cash into casino ripoffs online. *The Independent (London)*, p. 7. Retrieved November 28, 2009, from http://www.independent.co.uk/news/suckers-pour-cash-into-casino-ripoffs-online-1287336.html.

Barrett, R.. (2004). *Show me the money: Foreign lottery scams hit the jackpot in the US*. Retrieved March 24, 2008. Online at http://www.consumerwebwatch.org/dynamic/fraud-investigation-show-me-the-money.cfm

Best, J.. Luckenbill, D.F.. (1982). *Organizing deviance*. Englewood Cliffs, NJ: Prentice-Hall.

Biever, C.. (2004, November 3). *How zombie networks fuel cybercrime*. NewScientist.com. Retrieved June 5, 2005, from http://www.newscientist.com/channel/info-tech/electronic-threats /dn6616.

Bogard, W.. (1996). *The simulation of surveillance: Hypercontrol in telematic societies*. Cambridge, UK: Cambridge University Press.

Bortz, B.. (2008). *LinkedIn: Bill Bortz*. Retrieved April 4, 2008, from http://www.linkedin.com/pub/4 /1BB/653.

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.

Brenner, S.W.. (2007). Cybercrime: Re-thinking crime control strategies. In Jewkes, Y.. (Ed.), *Crime online*. Cullompton: Willan.

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

Brown, S.. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 190 (2), 233–244.

Brunker, M.. (2004, September 21). *Poker "bots" raking online pots?* Retrieved March 20, 2008, from http://www.msnbc.msn.com/id/6002298/print/1/displaymode/1098/.

Bullough, O.. (2004, July 28). Police say Russian hackers are increasing threat. *USA Today*. Retrieved April 5, 2008, from 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, from http://www.sportshandicappingforum.com /showthread.php?t=56569.

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

Cassavoy, L.. (2005, August 24). Web of crime: Internet gangs go global. *PC World*. Retrieved October 25, 2005, from http://www.pcworld.com/article/122242 /web_of_crime_internet_gangs_go_global.html.

Cere, R.. (2007). Digital undergrounds: Alternate politics and civil society. In Jewkes, Y.. (Ed.), *Crime online*. Cullompton: Willan.

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.

Computer Crime Research Center (CCRC). (2005, May 11). *U.S. cyber-crime unit focuses on Russian hackers*. Retrieved May 21, 2005, from http://crime-research.org/analytics/1226.

Computer Emergency Response Team — Laboratoire d'Expertise en Sécurité Informatique (CERT-LEXSI). (2006). *Online gaming cybercrime: CERT-LEXSI'S White Paper*, July 2006.

Costigan, C.. (2007, October 20). *Online gambling: Hacking by Costa Rican employees not uncommon*. Retrieved March 23, 2008, from http://www.gambling911.com/online-gambling-102007.html.

Council of Europe. (2005). Summary of the Organized Crime Situation Report 2004: Focus on the threat of cybercrime. *Trends in Organized Crime*, 8 (3), 41–50.

Department of Justice (DOJ). (2006, May 17). *Money laundering indictment unsealed against major Internet gambling site operators, alleges $250 million in online wagers*. Retrieved April 2, 2008, from http://www.usdoj.gov/opa/pr/2006/May/06_crm_298.html.

Department of Justice (DOJ). (2007a). *Man sentenced to 34 months in prison for involvement in large identity-theft ring*. Retrieved June 1, 2010, from http://www.justice.gov/usao/nys /pressreleases/January07/elekedesentencingpr.pdf

Department of Justice (DOJ). (2007b, November 14). Statement of Catherine Hanaway, United States Attorney, Eastern District of Missouri, United States Department of Justice. Before the United States House of Representatives Committee on the Judiciary Concerning "Internet Gambling." Retrieved June 1, 2010, from http://judiciary.house.gov/hearings /pdf/Hanaway071114.pdf

District Attorney Queens County. (2008, February 7). *Twenty-six charged in $10 million dollar Gambino organized crime family gambling, loan sharking and prostitution operation*. Retrieved May 15, 2009, from http://www.queensda.org/newpressreleases/2008/february /corozzo_02_07_2008_cmp.pdf

elGordo.com. (2008). *Advice about scams*. Retrieved April 4, 2008, from 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, from http://www.savemyos.com/organization/Additinal_PDF_files_files/Phishing-dhs-report.pdf.

Ferentzy, P.. Turner, N.. (2009). Gambling and organized crime — A review of the literature. *Journal of Gambling Issues*, 23, pp. 111–155.

Finch, E.. (2007). The problem of stolen identity and the Internet. In Jewkes, Y.. (Ed.), *Crime online*. Cullompton: Willan.

Gambling Magazine. (1999). *The real danger for this industry*. Retrieved October 19, 2006, from http://gamblingmagazine.com/articles/starnet/starnet113.htm.

Games and Casino. (2006). *Blacklisted casinos*. Retrieved February 2, 2007, from http://www.gamesandcasino.com/blacklist.

Geiss, G.. Brown, G.C.. Pontell, H.N.. (2009). Internet gambling. In Schmalleger, F.J.. and Pittaro, M.. (Eds.), *Crimes of the Internet*. New York: Prentice-Hall.

Germain, J.M.. (2003, September 27). Computer viruses and organized crime: The inside story. *TechNewsWorld*. Retrieved November 10, 2005, from http://www.technewsworld.com/story/31679.html.

Germain, J.M.. (2004, March 23). Global extortion: Online gambling and organized hacking. *MacNewsWorld*. Retrieved May 21, 2005, from http://www.macnewsworld.com/story/33171.html

Giacopassi, D.. Pitts, W.J.. (2009). Internet gambling: The birth of a victimless crime. In Schmalleger, F.J.. and Pittaro, M.. (Eds.), *Crimes of the Internet*. New York: Prentice-Hall.

Ginsberg, A.. (2009, April 24). Brooklyn judge denies prosecutor's request to isolate Nicholas Corozzo in jail. *New York Post*. Retrieved May 15, 2009, from http://www.nypost.com/devon/07242009/news

Goldman, R.. (2007, October 19). Online poker players expose alleged fraud. *ABCNews.com*. Retrieved January 29, 2008, from http://abcnews.go.com/print?id=3752500.

Golubev, V.. (2005, March 16). *DoS attacks: Crimes without penalty*. Computer Crime Research Center (CCRC). Retrieved June 5, 2005, from http://www.crime-research.org/articles/1049/.

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, 104–118.

Grabosky, P.. (2001). Virtual criminality: Old wine in new bottles. *Social and Legal Studies*, 10 (2), 243–249.

Gray, P.. (2005, March). Hackers: The winds of change. *Secured Newsletter*. Retrieved June 5, 2005, from http://www.iss.net/newsletters/secured/2005/mar/winds_of_change.html

Griffiths, M.D.. Parke, J.. (2004). Gambling on the Internet: Some practical advice to give clients. *Journal of Gambling Issues*, 11.

Griffiths, M.D.. Parke, A.. Wood, R.T.A.. Parke, J.. (2006). Internet gambling: An overview of psychosocial impacts. *Gaming Research and Review Journal*, 27 (1), 27–39.

Gu, Q.. Liu, P.. Chu, C.. (2004). *Hacking techniques in wired networks*. Retrieved March 23, 2008, from http://ist.psu.edu/s2/paper/hack-wired-network-may-04.pdf.

Heinrichs, P.. (2001, September 30). Beware of the dot con artists. *The Sunday Age*, p. 6.

Hintze, H.. (2008). *Compensation resumes in UltimateBet scandal as legal agreement reached*. Retrieved November 4, 2008, from http://www.pokernews.com/news/2008/11/ultimate-bet-scandal.htm.

HoldemGenius. (2008b). *Software updates — Holdem Genius*. Retrieved April 2, 2008, from http://www.holdemgenius.com/software-updates.html.

Holt, T.J.. (2009). Lone hackers or group crackers: Examining the social organization of computer hackers. In Schmalleger, F.J.. and Pittaro, M.. (Eds.), *Crimes of the Internet*. New York: Prentice-Hall.

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 June 1, 2010, from http://216.92.206.5/online/IGDA_WebDL_Whitepaper_2004.pdf

Jellenc, E.. Zenz, K.. (2007). *Global threat research report: Russia*. Retrieved June 1, 2010, from http://www.verisign.com/static/042139.pdf.

Jewkes, Y.. (Ed.). (2003). *Dot.cons: Crime, deviance and identity on the Internet*. Cullompton: Willan.

Jewkes, Y.. (Ed.). (2007). *Crime online*. Cullompton: Willan Publishing.

Jewkes, Y.. Andrews, C.. (2007). Internet child pornography: International responses. In Jewkes, Y.. (Ed.), *Crime online*. Cullompton: Willan.

Johnston, L.. Shearing, C.. (2003). *Governing security: Explorations in policing and justice*. New York: Routledge.

Karshmer, A.. (2005). Virtual villains: Global gangsters are extorting money from online casinos with a novel threat: we'll spam you to death. *MSNBC*. Retrieved June 1, 2010, from http://www.newsweek.com/id/54694

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 June 1, 2010, from http://articles.sun-sentinel.com/1997-09-08/news/9709070222_1_online-casino-online-gambling-internet-gambling

Kelley, R.. Todosichuk, P.. Azmier, J.J.. (2001). *Gambling @ Home: Internet gambling in Canada*. Calgary: Canada West Foundation.

Kahnawake Gaming Commission (KGC). (2008a). *In the matter of Absolute Poker: Investigation regarding complaints of cheating (May 29)*. Kahnawake Mohawk Territory.

Kahnawake Gaming Commission (KGC). (2008b). *Kahnawake Gaming Commission imposes sanctions on UltimateBet with regard to cheating incidents (September 29)*. Kahnawake Mohawk Territory.

Kahnawake Gaming Commission (KGC). (2009). *In the matter of Tokwiro Enterprises ENRG, carrying on business as UltimateBet. Investigation regarding complaints of cheating (September 11)*. Kahnawake Mohawk Territory.

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.

Kvarnstrom, H.. Lundin, E.. Jonsson, E.. (2000). *Combining fraud and intrusion detection — Meeting new requirements*. Retrieved March 10, 2007, from http://www.ce.chalmers.se/~emilie/papers/Kvarnstrom_nordsec2000.pdf.

Lemieux, V.. (2003). *Criminal networks*. RCMP. Retrieved June 1, 2010, from http://dsp-psd.pwgsc.gc.ca/Collection/JS62-107-2003E.pdf

Levitt, S.D.. (2007, October 17). The Absolute Poker cheating scandal blown wide open. *The New York Times*. Retrieved January 29, 2008, from http://freakonomics.blogs.nytimes.com/2007/10/17/the-absolute-poker-cheating-scandal-blown-wide-open/.

Leyden, J.. (2006, October 4). Russian bookmaker hackers jailed for eight years. *The Register*. Retrieved March 24, 2009, from http://www.theregister.co.uk/2006/10/04/russian_bookmaker_hackers_jailed/.

Leyden, J.. (2008, February 28). Phishers clean up at online casinos. *The Register*. Retrieved February 28, 2009, from http://www.theregistrar.co.uk/2008/02/28/casino_phishing/.

Mann, D.. Sutton, M.. (1998). Netcrime: More change in the organization of thieving. *British Journal of Criminology*, 38 (2), 201–228.

Mark, R.. (2007, January 25). *BetonSports ID thief sentenced to 34 months*. Retrieved April 3, 2008, from http://www.insideid.com/print.php/3656181.

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

Maxfield, M.G.. Babbie, E.. (2001). *Research methods for criminal justice and criminology*. Belmont, CA: Wadsworth.

McAfee. (2005). *McAfee Virtual Criminology Report: North American study into organized crime and the Internet*. Retrieved October 20, 2005, from http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf.

McAfee. (2007). *McAfee North America Criminology Report: Organized crime and the Internet 2007*. Retrieved January 21, 2008, from http://us.mcafee.com/en-us/local/html/identity_theft/NAVirtualCriminologyReport07.pdf.

McConnell International LLC. (2000). *Cybercrime … and punishment? Archaic laws threaten global information*. Retrieved June 1, 2010, from http://www.witsa.org/papers/McConnell-cybercrime.pdf

McMillen, J.. Grabosky, P.. (1998). *Internet gambling: Trends and issues in crime and criminal justice No 88*. Canberra: Australia Institute of Criminology. Retrieved December 9, 2007, from http://www.aic.gov.au/documents/0/B/0/%7B0B0D75F4-B63C-41DC-BD31-63FC2D90C9A9%7Dti88.pdf.

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.L.. Perrier, D.. (2007). The security of gambling and gambling with security: Hacking, law enforcement and public policy. *International Gambling Studies*, 7 (1), 43–58.

McMullan, J.. Rege, A.. (2007). Cyber-extortion at online gambling sites: Criminal organization and legal challenges. *Gaming Law Review*, 11 (6), 648–665.

Moore, R.. (2007). The role of computer forensics in criminal investigations. In Jewkes, Y.. (Ed.), *Crime online*. Cullompton: Willan.

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. *Infoconomy*. Retrieved June 1, 2010, from http://www.information-age.com/articles/287926/locked-out.thtml

Moses, A.. (2008, September 30). Aussie exposes online poker rip-off. *Sydney Morning Herald*. Retrieved November 21, 2008, from http://www.smh.com.au/news/biztech/dogged-aussie-detective-work-reveals-10m-ripoff/2008/09/30/1222651059903.html.

Murphy, A.. Pender, A.. Reilly, L.. Connel, S.. (2005). *Denial of service and countermeasures*. Networks and Telecommunications Research Group. Retrieved May 21, 2005, from http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group2/.

Naraine, R.. (2006, May 17). Rootkit infiltrates online poker software. *eWeek.com*. Retrieved March 21, 2008, from http://www.eweek.com/c/a/Security/Rootkit-Infiltrates-Online-Poker-Software/.

Neuman, L.W.. (2003). *Social research methods: Qualitative and quantitative approaches*. Boston, MA: Allyn & Bacon.

Nhan, J.. Huey, L.. (2008). Policing through nodes, clusters and bandwidth. In Leman-Langlois, S.. (Ed.), *Techno crime: Technology, crime and social control*. Cullompton: Willan.

North Country Gazette (2006, November 15). Massive Internet gambling operation busted. Retrieved March 20, 2008, from http://www.northcountrygazette.org/articles/111506InternetGambling.html

North Country Gazette (2008, February 7). Gambino captain, others busted for sports gambling. Retrieved May 15, 2009, from http://www.northcountrygazette.org/2008/02/07/gambino-captain-others-busted-for-sports-gambling/.

Nuttall, C.. (2004, February 23). Hackers blackmail internet bookies: Criminals believed to be targeting Grand National. *Financial Times*. Retrieved May 21, 2005, from http://www.toplayer.com/pdf/FinancialTimes_230204.pdf.

Online-Casinos.com. (2008). *DDOS danger for online gambling sites*. Retrieved April 3, 2008, from 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, from http://www.onlinepoker-news.com/20070906/bots_are_used_to_launder_money_in_online_ich.aspx

Parke, J.. Rigbye, J.. Parke, A.. Wood, R.T.A.. Sjenitzer, J.. Vaughan Williams, L.. (2007). The 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 (e COGRA). Retrieved November 24, 2008 from http://www.ecogra.com/Downloads/eCOGRA_Global_Online_Gambler_Report.pdf

Paulson, R.A.. Weber, J.E.. (2006). Cyber-extortion: 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 Curriculum Development Conference, September 23–24, 2005.

Penenberg, A.L.. (1998, June 12). Gambler beware. *Forbes Digital Tool: E-Business*. Retrieved June 1, 2010, from http://www.forbes.com/1998/06/12/feat.html.

Polson, S.. (2008, November 6). *UltimateBet, Absolute owner reaches settlement*. Retrieved December 12, 2008, from http://www.pokerlistings.com/ultimatebet-absolute-owner-reaches-settlement-32573.

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, from http://www.prnewswire.co.uk/cgi/news/release?id=63585.

Public Broadcasting Service. (2001). *Interview: Chris Davis*. Retrieved October 15, 2007, from http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/davis.html

Queen, L.. (2007). *Smart Scarborough senior avoids lottery scam*. Retrieved June 1, 2010, from http://www.insidetoronto.com/article/46815–smart-scarborough-senior-avoids-lottery-scam

Ratliff, E.. (2005, October 10). The zombie hunters: On the trail of cyberextortionists. *The New Yorker*. Retrieved June 1, 2010, from http://www.newyorker.com/archive/2005/10/10/051010fa_fact

Reuters News Service. (2001). *Hackers win high stakes at gambling sites*. Retrieved June 1, 2010, from http://news.cnet.com/news/0-1005-200-7119198.html?tag=cd_mh

Rogers, M.K.. (2005). *The development of a meaningful hacker taxonomy: A two dimensional approach*. Retrieved January 23, 2007, from https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2005-43.pdf

RSeconsulting. (2006, October). *A literature review and survey of statistical sources on remote gambling. Final report*. Retrieved October 7, 2006 from http://www.culture.gov.uk/reference_library/publications/3487.aspx.

Schmalleger, F.J.. & Pittaro, M.. (Eds.). (2009). *Crimes of the Internet*. New York: Prentice-Hall.

Shaw, C.. (2004, September 13). Net surfing more than working? Websense cuts down on misuse. *Investor's Business Daily*, National Edition, p. B02.

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, 489–506.

Skoudis, E.. (2007, July 24). *What are the risks of logging into a botnet control channel?* Retrieved October 31, 2007, from http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1274217,00.html.

Smed, J.. Knuutila, T.. Hakonen, H.. (2006). *Can we prevent collusion in multiplayer online games?* Retrieved January 10, 2007, from http://www.stes.fi/scai2006/proceedings/168-175.pdf

Smith, G.. Wynne, H.. (1999). *Gambling and crime in Western Canada: Exploring myth and reality*. Calgary: Canada West Foundation.

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

Sturgeon, W.. (2005, May 18). *Online gamblers targeted by scams*. Retrieved March 26, 2007, from 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, from http://www.realtime-websecurity.com/articles_and_analysis/2007/10/botnets_meet_oceans_eleven_sca.html.

Swoboda, E.D.. (2008). Muddy Waters. Retrieved June 1, 2010, from http://www.igamingnews.com/index.cfm?page=artlisting&ContentId=189844

Symantec. (2007). *Symantec Internet security threat report: Trends for January–June 2007*. Retrieved October 31, 2007, from http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf

Taylor, M.. Holland, G.. Quayle, E.. (2001). Typology of paedophile picture collections. *The Police Journal*, 74, 97–107.

Thompson, I.. (2007). *Phishing attacks target PartyPoker*. Retrieved March 20, 2008, from http://www.vnunet.com/vnunet/news/2183974/phishing-attack-targets-party.

Times of India. (2008, January 20). Nigerian arrested for online fraud. *Times of India*. Retrieved April 4, 2008, from http://timesofindia.indiatimes.com/Cities/Mumbai /Nigerian_arrested_for_online_fraud/articleshow/2714862.cms.

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

Ulick, A.. (2007, December 24). *Josh “JJProdigy” Fields asks poker world for forgiveness*. Retrieved April 3, 2008, from http://www.tightpoker.com/news/Josh-JJProdigy-Fields-Asks-Forgiveness.shtml.

United States Attorney Southern District of New York (USASDNY). (2005). *U.S. indicts 17 in massive crackdown on multi-million dollar illegal gambling operation*. Retrieved September 24, 2007, from http://www.usdoj.gov/usao/nys/pressreleases/January05/uvarietalindictmentpr.pdf

United States Attorney Southern District of New York (USASDNY). (2008). *Former Internet gambling site employee pleads guilty to stealing identities for international identity theft ring*. Retrieved June 1, 2010, from http://www.justice.gov/usao/nys/pressreleases/September08 /kalonjipleapr.pdf.

Venezia, T.. Martinez, E.. Livingston, I.. (2006). $3.3 Bil Casino Royale: ‘Net Bet King of Qns. In ‘Biggest Ever’ Bookie Bust. *The New York Post*. Retrieved April 2, 2008, from http://www.nypost.com/p/news/bust_casino_royale_net_bet_king_EIkJFy6LMixfeTga2RyxBP

Walker, C.. (2004). *Russian Mafia extorts gambling Websites*. Retrieved November 10, 2005, from http://www.americanmafia.com/Feature_Articles_270.html

Wall, D.. Williams, M.. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology and Criminal Justice*, 7, 391–415.

Wall, D.S.. (2007). *Cybercrime: The transformation of crime in the information age*. London: Polity Press.

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

Williams, M.. (2006). *Virtually criminal: Crime, deviance and regulation online*. New York: Routledge.

Williams, P.. (2002). *Organized crime and cybercrime: Synergies, trends, and responses*. Retrieved January 19, 2006, from http://crime-research.org/library/Cybercrime.htm.

Williams, R.J.. Wood, R.T.. (2007, August 31). *Internet gambling: A comprehensive review and synthesis of the literature*. Report prepared for the Ontario Problem Gambling Research Centre, Guelph, ON.

Williams, R.J.. Wood, R.T.. (2009), *Internet gambling setting the stage: History, current world wide situation, regulatory frameworks and concerns with Internet gambling*. Paper presented at Alberta Gaming Research Institute Conference, March 2009.

Wood, R.T.. Williams, R.J.. (2009, January 5). *Internet gambling: Prevalence, patterns, problems and policy options*. Final Report prepared for the Ontario Problem Gambling Research Centre, Guelph, ON.

Wood, R.T.. Williams, R.J.. Lawton, P.. (2007). Why do Internet gamblers prefer online versus land-based venues?*Journal of Gambling Issues*, 20, 235–250.

Wood, R.T.A.. Griffiths, M.D.. (2008). Why Swedish people play online poker and factors that can increase or decrease trust in poker web sites: A qualitative investigation. *Journal of Gambling Issues*, 21, 80–97.

Woods, D.. Coats, G.. (2008). *Is online poker safe?* Retrieved November 21, 2008, from http://www.inside-edge-mag.co.uk/pokerlife/pokerfeatures/7815.

World Poker Rules (WPR). (2007). *Sorel Mizzi & Chris Vaughn: A dissenting opinion*. Retrieved March 25, 2008, from http://www.worldpokerrules.com/news.php?id=368.

Yan, J.. (2003). *Security design in online games*. Retrieved June 1, 2010, from http://www.acsac.org/2003/papers/114.pdf.

Yan, J.. Randell, B.. (2005). *A systematic classification of cheating in online games*. NetGames'05. Retrieved March 10, 2007, from http://www.research.ibm.com/netgames2005/papers/yan.pdf.

Zacharias, J.. (2004). *Internet gambling: Is it worth the risk?* Retrieved March 20, 2007, from http://www.bcresponsiblegambling.ca/other/docs/internet_gambling_jan_zacharias.pdf

Zangeneh, M.. Griffiths, M.. Parke, J.. (2008). The marketing of gambling. In Zangeneh, M.. , Blaszczynski, A.. & Turner, N.. (Eds.), *In the pursuit of winning: Problem gambling theory, research and treatment* (pp. 135–153). New York: Springer.

ZDNet. (2005, April 6). *Russian hackers "the best in the world"* Retrieved April 5, 2008, from http://news.zdnet.co.uk/security/0,1000000189,39193999,00.htm?r=1

Article Categories:

- Research

Keywords:
crime
,
Internet
,
gambling
.

Related Article(s):