Online gambling and crime: a sure bet?

BANKS, James

Published version

BANKS, James (2012) Online gambling and crime: a sure bet? The ETHICOMP Journal.

ONLINE GAMBLING AND CRIME: A SURE BET?

Dr James Banks
Senior Lecturer in Criminology, Department of Law, Criminology and Community Justice, Sheffield Hallam University, Sheffield, UK

Despite a growing body of research that is exploring the deleterious social effects of online gambling, there has, to date, been very little empirical research into internet gambling and crime. This paper seeks to initiate discussion and exploration of the dimensions of crime in and around internet gambling sites through an analysis of the current literature on gambling online. The paper forms part of a wider study that seeks to examine online gambling related crime and identify appropriate legal, technological and educational frameworks through which to limit victimisation.

1. Introduction

The explosive growth of the internet as a public and commercial vehicle has provided new opportunities for gambling based activities to take place online. Facilitated by the development of the first gambling software, by Microgaming in 1994, and encrypted communication protocols which enable online monetary transactions, by Cryptologic in 1995, Antiguan based company InterCasino became the first internet gambling site to accept an online wager in January 1996 (Williams and Wood 2007). By the end of that year, approximately 15 sites were accepting wagers, rising to 200 by the end of 1997, 650 by the end of 1999 and 1,800 by the end of 2002 (Schwartz 2006). Today, there are in the region of 2,347 listed gambling sites in existence, including 768 casinos, 524 poker rooms, 430 sportsbooks, 19 betting exchanges, 377 bingo sites, 45 skill games sites, 94 lottery sites, 13 backgammon sites and 16 mahjong and rummy sites (Casino City 2010). These sites are spread across 661 owners who operate out of 74 jurisdictions, including Antigua and Barbuda, Australia, Costa Rica, the Dutch Antilles, the Kahnawake Mohawk reserve in Canada, Malta and the United Kingdom (Williams and Wood 2007, 2009; Casino City 2010).

The marked growth in online gambling sites appears to stem from a number of inter-related factors (Griffiths and Parke 2002; Watson, Liddell, Moore and Eshee 2004). First, online gambling offers an extremely lucrative business venture for many. The entertainment and leisure industry has recognised the cost effectiveness of online gambling sites, as start-up and operating costs are considerably lower than those of their land-based counterparts. For example, operating a land-based casino could require thousands of staff and an outlay of around £300 million, yet an internet gambling business can be run for less than one per cent of this investment (Clarke and Dempsey 2001). Moreover, the online gambling market represents one of the fastest growing segments of the gambling industry (Summerfield and Loo 2010). Despite political and legislative restrictions within certain jurisdictions, the online gambling market recorded record revenues totalling US$21.2 billion in 2008 and this is expected to grow by 42 per cent to US$30 billion by 2012 (H2 Gambling Capital 2009).

Second, significant sectors of the world populace have the potential to access online gambling sites. With computers becoming less expensive, simpler to use and more readily available, the opportunity for consumers to partake in anonymous and effortless gambling from the comfort of their own home or workplace has increased substantially (Keller 1999; Kish 1999). The actual number of people gambling online is difficult to identify, but it has been estimated that over 14 million have used internet gambling sites (American Gaming Association 2006; RSeConsulting 2006). Of this figure, 4 million are US citizens, 3.3 million are from Europe and 7 million are from the Asia-Pacific Region. And whilst the prevalence of online gambling amongst the general population is low, it continues to grow. In 1999, the British Gambling Prevalence Study recorded that 0.2 per cent of UK adults had gambled online (Sproston, Erens and Orford 2000). By 2007, this figure had risen to 6 per cent, representing a 2900 per cent increase within the intervening period (Wardle et al., 2007).

Third, internet gambling services have continued to enhance the consumer's online experience. The development of sophisticated gambling software that combines live remote wagering and increasing realism with multi-lingual websites has made gambling online an appealing alternative to land-based gambling operations (Griffiths and Parke 2002). Furthermore, integrated, multicurrency e-cash systems and superior customer services continue to improve the safety, legitimacy and reputation of online gambling amongst consumers.

In sum, the online gambling experience is likely to continue to be desirable to consumers because it offers frequent and interactive gambling that is characterised by accessibility, affordability and anonymity. Moreover:

> As the popularity of both gambling and online entertainment continues to grow, the online gaming market is without doubt an attractive area of expansion for software developers, casinos and other land-based gambling operators, related suppliers, and industry newcomers and investors alike. (Summerfield and Loo 2010: 16)

Nevertheless, the development of such technologies has not been accepted uncritically. The last decade has witnessed a growing body of research that has explored the deleterious social effects of online gambling. Of particular concern is the ease with which young people and other vulnerable populations can access online gambling sites (Griffiths 1995; Smeaton, Poole, Chevis and Carr 2004), increases in gambling, money spent gambling, problem gambling and gambling addiction (Griffiths 2003), public health and public safety (Griffiths 2004). Yet, to date, there has been very little empirical research into internet gambling and crime (McMullan and Rege 2010). This is surprising given that the scale and density of internet gambling sites, the voluminous number of players and the large quantities of e-cash available as tournament prizes or held in online gambling accounts, provides a marketplace replete with criminal potential. Nevertheless, little is known about the frequency, types, techniques and organisational dynamics of internet gambling related crime nor has there been any consideration of the degree to which such

crimes go undetected. This paper seeks to initiate discussion and exploration of the dimensions of crime in and around gambling sites through an analysis of the current literature on gambling online. Although much of this work does not explicitly set out to examine crime online, it enables an initial assessment of the forms and features of crimes that take place in and around internet gambling sites. Moreover, the paper identifies the opportunities and complexities in undertaking empirical research and outlines a research agenda that will help shape this field of study.

2. Crime Online

Cyberspace has been depicted as a 'world wild west', with the threat of e-criminality looming large over an increasingly globalised world (Sandywell 2010). The significant quantities of e-cash held in online gambling sites and flowing between them and various ancillary organisations presents a digital network ripe for criminal exploitation. In such contested spaces, gambling site operators, employees, customers and unwanted 'third parties' anonymously intermingle, creating the opportunity for multi-various forms of criminal activity and constructing rhyzomatic relations between perpetrators and victims.

McMullan and Rege's (2010) research suggests that online 'criminal entrepreneurs' range from solo actors to dynamic, amorphous and loosely connected assemblages who engage in singular, but often substantial, crimes in and around online gambling sites. In McMullan and Rege's typology, three distinct categories of 'criminal entrepreneur' that exhibit various levels of skill and sophistication are identified. 'Cybernomads', solo criminal actors, differ in their skills, motivations and technological acumen, but typically either purchase or manufacture 'toolkits' that enable individuals to cheat and steal from online gambling sites and their clientele. More advanced cybernomads, often akin to professional criminals, engage in the production of malware, technical intelligence and personal information that can be sold on to others through the underground economy. Alternatively, advanced hackers may execute their own attacks on gambling sites or subcontract their services to other criminal groups. By contrast, 'dot.con teams' may consist of small-scale organised crime groups, players, consultants or web and gambling site owners, managers and employees who unite to commit acts of fraud, theft or money laundering. Online players may collude with other players to cheat opponents or engage with gambling site insiders who provide privileged information that enables the committal of crimes against both employers and their clientele. Moreover, organised crime groups often utilise online gambling sites to launder money and 'clean' their proceeds from various criminal activities. Finally, 'criminal assemblages' consist of dynamic and complex criminal networks that engage in ongoing extortion, phishing, identity fraud and money laundering enterprises. More formal and continuous than Dot.con teams, the scale, intensity and duration of their criminal activity means criminal assemblages are more likely to be identified by corporate and government agencies who become involved in 'techno wars' with criminal groups as they seek to limit crime and victimisation visited upon online gambling communities.

In short, internet gambling sites can operate as source of criminal activity, as a vehicle for crime or support for other criminal enterprise. Criminal entrepreneurs

may target gambling operations and/or their clientele or utilise gambling sites as a conduit for crime. Moreover, in order to engage in fraudulent activities, criminal entrepreneurs may enlist gambling organisations, their employers and clientele or disguise themselves as legitimate online gambling operations or customers. Similarly, legitimate gambling businesses may employ corrupt practices as profits turn to losses and once genuine patrons may seek to engage in criminal practices in order to reduce their deficits. Nevertheless, this dense tangle of virtual villains and victims can be simplified to identify four distinct forms of e-crime and modus operandi of gambling site operators and their employees, users of online gambling sites and criminal entrepreneurs, who either utilise gambling sites as a conduit for nefarious activities or specifically target gambling operators and their clientele. It is to this typology that discussion now turns.

3. Typology

3.1 *Fraud*

Ensuring that online gambling is conducted fairly and openly is a significant challenge for the gambling industry. Characterised by low profit margins and high percentage payouts, which are estimated at between 88 and 98.7 per cent of turnover (RSeconsulting 2006), online gambling sites must sustain a high turnover if they are to be successful. In a highly competitive market, the reputation of operators may be considered paramount as players are likely to switch to rival sites if gaming practices are deemed questionable. Yet low levels of consumer trust in online gambling operations and the fairness of their games does not appear to equate to a reduction in website usage (Haried 2009). This is surprising given that the limited regulation of online gambling, coupled with the multi-jurisdictionality of online gambling sites, provides significant opportunities for unscrupulous gambling operators to engage in fraudulent activities.

Unsurprisingly, there are many cases in which online sites have not paid winnings, cheated players with unfair games or absconded with player's deposits (Games and Casino 2006). Sportsbookreview (2010), an independent monitoring organisation, details a 'black list' of 507 online gambling sites and an 'avoid list' of 555 online operators who have experienced problems ranging from bonus scams to financial collapse. Bookmakers listed include those who are not licensed to operate a gambling company where required, have had payout problems in the past, used bonus confiscation and scam tactics, are illegally hosted in the US, been involved in wager scams, unjustly cancelled bets, changed rules after a wager or are part of an operation which has had such issues in the past.

In its simplest form, fraud often involves gambling sites who take gambler's money but do not pay any winnings (Griffiths 2010). The lack of online gambling regulation in many countries means that it is possible to launch a site, collect customer data and banking details, take bets and then close the site before paying out any winnings (McMullan and Rege 2007). These 'deposit-only bookmakers' regularly appear on the market and eventually disappear. Offering generous sign-up bonuses to entice customers, such sites operate from domain registrations which are

hidden behind ‘domains by proxy’, which make it unclear as to who owns the site and whether or not they are licensed.

Such websites are often adorned with kite-marks of 'social responsibility' that suggest the business is government licensed or has been subject to third party accreditation. The display of logos from organisations such as the Gambling Commission, the Independent Betting Adjudication Service, Gamcare and Gambling Therapy help make such sites look safe, reputable and trustworthy. Criminal enterprises also create immaculate forgeries of legitimate gambling sites by ‘lifting’ the general design, graphics and materials from such sources (Griffiths 2004; McMullan and Rege 2007). These state of the art webpage forgeries are one of the most common fraudulent practices that fool unsuspecting customers into depositing their money.

The fragile nature of online gambling businesses also means a decrease in turnover can result in once legitimate companies engaging in corrupt practices. For example, BetOnSports, based in Costa Rica, formerly one of the largest online gambling firms with an annual turnover of US$1.8 billion, was closed down with executives charged with racketeering, conspiracy and fraud (McCarthy 2006; Salter 2009). The company misled gamblers into believing its operations were legal and that their money was safe and accessible when instead the money was being used to expand operations and purchase a rival firm. When BetOnSports ceased trading in 2006, customers lost over US$16million in unpaid deposits and winnings (Salter 2009). More recently, the managing director of Maltese based sportsbook Strykke was arrested after failing to pay over US$70,000 to customers and operating without an appropriate licence (Sportsbookreview 2010).

Other ‘legitimate’ operators employ more sophisticated forms of entrapment which provide an air of legitimacy to their techniques to defraud customers. Complex terms of agreement and wager requirements prevent customers withdrawing their money and many find their winnings and deposit locked inside an account until all funds are exhausted. For example, one bookmaker offers to match customer’s deposits to the tune of £200. However, customer's money may only be withdrawn after the deposit and bonus have each been wagered six times at odds of 2.0 or more. The difficulty for customers is that their bonus can only be bet once all other funds have been wagered. This requires a customer who wins with his first bet to wager both his original stake and any winnings on a second bet before he can bet with his bonus. The greater the winnings the more money a customer must bet through before he can bet with his bonus. Requiring a minimum of twelve bets – wagering the full deposit (and any winnings) followed by the bonus – before a withdrawal may be sanctioned it is highly unlikely that the player will escape with any money.

There are also a number of cases in which legitimate customers have been defrauded by other online gamblers who operate alone or in partnership with other players or employees of online gambling operators. Online poker appears to be particularly susceptible to deceptive player practices. This may involve the collusion between poker players at the same table (i.e. several players are actually in the same room using different computers) or the use of computer programs using optimal play

(poker bots) against other players (Brunker 2004). Many of those who are victims of such practices remain completely unaware of any wrongdoing considering their loss to be the result of meeting a more skilled (or more fortunate) opponent.

3.2 *Theft*

The theft of customer's money is at heart of many of the fraudulent activities undertaken by both criminal entrepreneurs and once legitimate gambling operations. However, there have been several cases of hackers altering online gambling sites to pay wins and enable the theft of funds from gambling site owners (Reuters 2001; RSeconsulting 2006). For example, in 2001, hackers enabled 140 gamblers to win over $1.9 million in only a few hours by altering the casino games of Cryptologic's operating licensees so that users could not lose.

The internet also offers a valuable opportunity for criminal entrepreneurs to disguise themselves and their identities through multiple aliases or the theft of an unsuspecting person's identity. Identity theft through a technique known as 'black-holing' has been targeted at users of online gambling web sites. Criminal entrepreneurs 'hijack' an online web site, surreptitiously redirecting customers to an identical looking site operated by the thieves. When the customer logs in, the criminals are able to collect their IDs and passwords. Passing the visitors straight through to the real website the thieves are then able to access the customers gambling account. Exploiting weaknesses in the DNS, which is at the core of the internet itself, gambling sites are vulnerable to such attacks irrespective of the internal defences the web site employs. Thus, as security analysts are quick to point out, there is no such thing as secure gambling software as skilled people in the hacking underground will always be able to exploit vulnerabilities in systems and steal money and information from gambling organisations (Gray 2005).

3.3 *Money Laundering*

It has been suggested by some (Mills 2001) that the potential for criminals to launder their ill-gotten gains through remote gambling sites is the greatest threat posed by the virtual gambling industry. Laundered funds can be the end product of successful criminal enterprise, but can also be employed to fund organised crime, terrorism, smuggling and counterfeiting, and this has led to significant attention from law enforcement agencies and their governments (Government Accountability Office 2002; RSeconsulting 2006). Yet whilst it is estimated that between US$300 billion and US$500 billion are laundered annually (Magliveras 1992; Barbot 1995; Sultzer 1995), the degree to which online gambling sites facilitate such activities is unclear. It is possible that the low limits on gambling, coupled with the close monitoring and recording of electronic financial transactions, effectively limit the opportunity for money laundering. Conversely, the high speed, high volume and international reach of online gambling operators and their clientele, alongside the anonymity afforded by the internet and encrypted payment processes, can make it difficult to trace payments. Moreover, gambling sites are frequently located in areas with weak or non-existent supervisory regimes, which may make them particularly susceptible to money laundering.

There are three principal ways in which gambling sites can theoretically be used to launder money: First, illegal funds may be transferred to a source inside the gambling organisation by gambling until all money is lost; second, illegal funds may be transferred from a casino insider to a gambler through the use of rigged games; third, casino gambling software may be programmed to respond to a specific password or sign-in command by removing a percentage of the money deposited and recording it as a gambling loss. Alternatively, legitimate gambling sites may be used by money launderers who operate a legitimate account under a false name. Individuals may 'clean' their illicit funds by wagering a small amount before withdrawing the remaining money or transferring it to an offshore account. Betting exchanges have also provided significant opportunity for the laundering of money, as all sides of an event may be bet on. Irrespective of the outcome and minus only the house 'vigorish', visible and declarable profits and losses can be generated.

As 'traditional' laundering requires the movement of illicit funds through financial institutions that are highly regulated, avoiding built-in detection processes is extremely challenging for the criminal entrepreneur. Yet the instantaneous and anonymous nature of the internet, augmented by the rapid development of both e-banking and the online gambling industry, has revolutionised the money laundering process and provided significant opportunity for launderers to deposit, cleanse and withdraw money, all at the click of a button. With no traditional financial institutions in place to alert authorities to potential criminal activity, ill gotten gains can be easily filtered into the stream of international commerce. So whilst the magnitude of this problem is, to date, unknown, the potential for money laundering is significant, given the laissez-faire approach to regulation in many of the jurisdictions in which online gambling occurs (Williams and Wood 2007).

3.4 *Extortion*

Cyberextortion presents a 'severe' threat to gambling organisations who seek to operate online (RSeconsulting 2006). The 'denial of service' (DoS) attack is a typical technique used in electronic extortion activities by crime syndicates who target internet gambling sites. DoS attacks occur when a network or server is inundated with thousands of requests that consume all available disk space, central processing unit time, bandwidth capability, or physical network components. Similarly, 'distributed denial of service' (DDoS) attacks originate from a group of compromised 'zombie' computers that flood systems with requests, overwhelming servers, crashing networks and shutting down sites. Attackers install software on zombie systems enabling them to be controlled by a master computer that directs a specific bandwidth assault against a chosen target. The infected zombie slaves form a 'botnet' that is herded into a single DDoS attack, which disrupts online gambling by denying access to the computer system for legitimate customers.

The business model for cyberextortion closely resembles that of the 'real world' racket, with criminal groups demanding payment from online organisations in order not to launch DoS attacks that will cripple their system and cost them many times more money in lost revenue (Lovet 2006). Threats are delivered via email to companies demanding the wiring of 'protection' money to a specific drop. If the company fails to make payment they are likely to be subject to an attack which

prevents or severely limits business operations. The success of online extortion is premised upon the extorted funds being clearly less than the potential loss caused by the down-time.

Occurring since 1999, the 21st century has seen a surge in DoS attacks against critical infrastructures and private businesses (Rege 2010). In the UK, the online gambling industry has been particularly susceptible to DoS attacks and extortion demands of between US$10,000 and US$50,000 from criminal gangs, particularly during big money-making events or games (Nuttall 2004). Betdaq, Totalbet, UKBetting and William Hill all recorded receiving extortion demands and being subject to attacks prior to the Cheltenham festival in 2004. Similarly, Irish bookmaker Paddy Power had its site paralysed for several hours during Super Bowl XXXVIII after failing to pay a ransom, whilst Canbet refused to meet a US$12,500 demand during the Breeders' Cup and was subject to a DDoS attack that made its servers inaccessible at a cost US$250,000 a day (Hess and Wrobleski 1996). Other companies have paid out thousands to cyberextortionists. In 2003, BoDog Sportsbook and Casino, who operate out of Costa Rica, met a ransom of US$20,000 after its website was shut down, whilst Antiguan based company BetWWWTS.com paid $30,000 to hackers after a DoS attack prevented thousands of customers placing wagers worth an estimated US$5 million (Rothman 2005; Paulson and Weber 2006).

The exact number and total cost of DoS attacks on online gambling sites is difficult to measure, particularly as gambling companies are likely to under-report such offences as they seek to maintain the integrity of their security systems and preserve the confidence of their clientele. However, security group Symantec detected an average of 1,402 DoS attacks per day suggesting they pose a significant threat to commercial businesses that operate online (Richards 2007). More specifically, server monitoring firm Netcraft examined the UK's top twenty betting sites and recorded 33 outages, across 15 sites, within a 14 day period (Ward 2004). Whilst half of the outages occurred late at night and are likely to be the result of routine maintenance, half of those logged occurred during the day and exhibited characteristics of a DoS attack, with servers struggling to deal with requests.

Clearly electronic extortion is a critical problem for the online gambling community as the cost of DoS attacks is likely to be significant for those failing to pay ransom demands. It is estimated that cyberextortionists cost British bookmakers alone $70 million in 2004 (Nuttall 2004). Thus, it appears that keeping gambling sites up and running is one of the biggest challenges facing online gambling operators.

4. Summary

Online gambling offers many opportunities for criminal entrepreneurs to engage in fraud, theft, extortion and money laundering in and around gambling sites. The large amounts of e-cash that circuit online gambling sites provide significant rewards for the dishonest. Yet, whilst this paper has highlighted some of the types, techniques and organisational dynamics of online gambling related crime, a number of significant gaps in knowledge remain.

In particular, little is known about the degree to which online gambling organisations and their clientele are victims of crime. An understanding of the extent to which online gamblers are victims of fraud and theft committed by gambling organisations is important if we are to develop appropriate safeguards and introduce effective regulatory regimes. Constructing suitable protection for consumers is surely a must if online gambling sites are to operate lawfully.

The societal effects of widespread access to online gambling have also yet to be explored. The links between gambling, problem gambling and pathological gambling have been subject to significant research (Griffiths and Parke 2002; Griffiths 2006; Hayer, Mayer and Griffiths 2009), but there has, to date, been little investigation into the degree to which public exposure to online gambling generates crime beyond the confines of the virtual world. In particular, online gambling amongst the young and vulnerable populations, the degree to which online gamblers commit crime to fund their habits, and the level of gambling associated violence (particularly domestic violence) need to be examined.

Ongoing assessment of anti-criminality measures is essential in order to mitigate the risk posed by the rapid (and largely uncontrolled) expansion of online gambling. There is, at present, very little cooperation and coordination between countries on remote gambling, coupled with a lack of symmetry in regulatory regimes. This lack of continuity will see online gambling organisations work out of 'regulation-light' jurisdictions and push customers towards unregulated sites. It is, therefore, essential that regulatory and policing frameworks are subject to rigorous assessment and appraisal.

Ultimately, the development of empirical research that explores online gambling, crime, policing and regulation is essential in order to help develop appropriate mechanisms to facilitate good governance and limit the effects of crime on online gambling organisations, their clientele and wider society.

References

American Gaming Association. (2006) *Gambling and the internet: The A.G.A. survey of casino entertainment.* Washington, DC: American Gaming Association.

Barbot, L. A. (1995) 'Money laundering: An international challenge', *3 Tulane Journal of International and Comparative Law*, 161, 190-193.

Brunker, M. (2004) *Are poker 'Bots' raking online pots?* online at http://www.msnbc.msn.com/id/6002298 accessed 14.12.2010.

Casino City (2010) *Online Casino City*, online at http://online.casinocity.com/ accessed 04.04.2011.

Clarke, R. and Dempsey, G. (2001) 'The feasibility of regulating gambling on the internet', *Managerial and Decision Economics*, 22, 1-3, 125-132.

Games and Casino (2010) *Blacklisted casinos*, online at http://www.gamesandcasino.com/blacklist.htm. accessed 14.12.2010.

Government Accountability Office (2002) *Internet gambling: An overview of issues*, GAO-03-89.

Gray, P. (2005) *Hackers: The winds of change*, online at www.iss.net 04.04.11.

Griffiths, M. D. (1995) *Adolescent gambling*. London: Routledge.

Griffiths, M. D. (2003) 'Internet gambling: Issues, concerns and recommendations', *CyberPsychology and Behaviour*, 6, 557-568.

Griffiths, M. D. (2004) 'Betting your life on it', *British Medical Journal*, 329, 1055-156.

Griffiths, M. D. (2006) 'An overview of pathological gambling' In: Plante, T. (ed) *Mental disorders of the new millennium*. New York: Greenwood: 73-98.

Griffiths, M. D. (2010) 'Crime and gambling: A brief overview of gambling fraud on the internet', *Internet Journal of Criminology*.

Griffiths, M. D. and Parke, J. (2002) 'The social impact of internet gambling', *Social Science Computer Review*, 20, 3, 312-320.

H2 Gambling Capital (2009) *eGaming Report*. London: H2 Gambling Capital.

Haried, P. (2009) 'Trust in the online gambling industry: We don't trust you, but please take our money', *Proceedings of ASBBS Annual Conference*, Las Vegas.

Hayer, T., Mayer, G. and Griffiths, M. D. (2009) *Problem gaming in Europe: challenges, prevention, and interventions*. New York: Springer.

Hess, K. M. and Wrobleski, H. M. (1996) *Introduction to Private Security*. Belmont, CA: Wadsworth.

Keller, B. P. (1999) 'The game's the same: Why gambling in cyberspace violates federal law', *The Yale Law Journal*, 108, 7, 1569-1609.

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.

Lovet, G. (2006) *Dirty money on the wires: The business models of cyber criminals*, Virus Bulletin Conference 2006, online at http://www.fortiguard.com/papers/VB2006_Dirty_Money_on_the_Wires.pdf accessed 14.12.2010.

Magliveras, K. D. (1992) 'Defeating the money launderer – The international and European framework', *Journal of Business Law*, March, 161-177.

McCarthy, M. (2006) 'U.S. cracking down on offshore betting industry', *USA Today*, online at http://www.usatoday.com/sports/2006-07-18-online-gaming_x.htm accessed 13.12.2010.

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

McMullan, J. L. and Rege, A. (2010) 'Online crime and internet gambling', *Journal of Gambling Issues*, 24, 5, 54-85.

Mills, J. (2001) 'Internet casinos: A sure bet for money laundering', *Journal of Financial Crime*, 8, 4, 365-383.

Nuttall, C. (2004) 'Hackers blackmail internet bookies: Criminals believed to be targeting Grand National', *Financial Times*, 23.02.2004.

Paulson, R. A. and Weber, J. E. (2006) 'Cyberextortion: An overview of Distributed Denial of Service Attacks against online gaming companies', *Issues in Information Systems*, 7, 2, 52-56.

Rege-Patwardhan, A. (2010) 'Cybercrimes against critical infrastructures: A study of online criminal organisation and techniques', *Criminal Justice Studies*, 22, 3, 261-271.

Reuters News Service (2001) *Hackers win high stakes at gambling sites*, online at http://mews.cnet.com/news/0-1005-200-7119198.html?tag=cd_mh accessed 12.12.2010.

Richards, J. (2007) 'Telegraph website targeted in mystery attack by hackers', *The Times Online*, online at http://technology.timesonline.co.uk/tol/news/tech_and_web/article1824601.ece accessed 14.12.2010.

Rothman, P. (2005) *Gambling sites prime DOS targets*, online at http://securitysolutions.com/mag/security_gambling_sites_prime/ accessed 14.12.2010.

RSeconsulting. (2006) *A literature review and survey of statistical sources on remote gambling*, Final Report, online at http://www.culture.gov.uk/reference_library/publications/34.87.aspx. accessed 31.10.2010.

Salter, J. (2009) *3 plead guilty in BetOnSports online gambling case*, online at http://www.physorg.comnews164995832.html accessed 13.12.2010.

Sandywell, B. (2010) 'On the globalisation of crime: The internet and new criminality', In Y. Jewkes and M. Yar (eds) *Handbook of Internet Crime.* Cullumpton: Willan: 38-66.

Saxena, R. (1998) 'Cyberlaundering: The next step for money launderers?', *10 St Thomas Law Review*, 685, 691.

Schwartz, D. G. (2006) *Roll the Bones: The History of Gambling*. New York: Gotham Books.

Smeaton, M., Poole, A., Chevis, A. and Carr, J. (2004) *Study into underage access to online gambling*, online at http://www.gamcare.org.uk/pdfs/StudyReportFinal.pdf accessed 29.03.2011.

Sportsbook Review (2010) *Worst Sportsbook List*, online at http://www.sportsbookreview.com/blacklist/ accessed 12.12.2010.

Sproston, K., Erens, B. and Orford, J. (2000). *Gambling Behaviour in Britain: Results from the British Gambling Prevalence Survey*. London: The National Centre for Social Research.

Sultzer, S. (1995) 'Money laundering: The scope of the problem and attempts to combat it', 63 *Tennessee Law Review*, 2, 3, 14-17.

Summerfield, M. and Loo, W. (2010) *Online Gaming: A Gamble or a Sure Bet?* London: KPMG International.

Ward, M. (2004) 'Bookies suffer online onslaught', *BBC News Online*, online at http://news.bbc.co.uk/1/hi/technology/3549883.stm accessed 29.03.2011.

Wardle, H., Sprotson, K., Orford, J., Erens, B., Griffiths, M., Constantine, R. and Pigott, S. (2007) *British Gambling Prevalence Survey 2007*.London: National Centre for Social Research.

Watson, S., Lidell, P. Moore, R. S. and Eshee, W. D. (2004) 'The legalization of internet gambling: A consumer protection perspective', *Journal of Public Policy and Marketing*, 23, 2: 209-213.

Williams, R. J. and Wood, R. T. (2007) *Internet Gambling: A Comprehensive Review and Synthesis of the Literature.* Report prepared for the Ontario Problem Gambling Research Centre, Guelph, ON.

Williams, R. J. and 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.