



RESEARCH SYNOPSIS

McMullan, J. L., & Rege, A. (2010). Online crime and internet gambling. *Journal of Gambling Issues*, 54-85. doi:10.4309/jgi.2010.24.5

RESEARCH QUESTIONS

What types of crimes occur at online gambling sites? How organized is online gambling crime? How effective is legal governance of online gambling crimes?

PURPOSE

Little research had been conducted on online crime and Internet gambling. The present study addressed this absence by conducting a qualitative investigation of the types, techniques, and organizational dynamics of online crime at the portals of Internet gambling sites.

PROCEDURE

A qualitative approach was taken to explore crimes/criminals associated with online gambling sites. Documents pertaining to online crimes/criminals (e.g., interviews, police reports, etc.) published between 2000 and 2008 were found via the Google search engine using 48 combinations of keywords (e.g., "cyberextortion and organized crime" and "player collusion and gambling", etc.). After eliminating duplicate documents, the researchers compiled approximately 500 documents.

KEY RESULTS

Cybernomads. Cybernomads and hackers were almost always solo criminal actors who stole or modified data, compromised computer systems, manipulated software for illegal purposes, or executed cyber attacks at online gambling sites. The profits were almost always consumed by the principal actor. Although cybernomads and hackers networked with people in order to obtain supplies, gain knowledge, plan strategies, and perfect attacks, they seemed to seldom need partners or to have come into much contact with their victims. These criminals varied with respect to their skills and motivations, but their strength was in their software and programming expertise. They lived ubiquitous online lives and constantly shifted from one Internet venue/ adventure to another, combining skill with bravado to cheat and steal and to frustrate detection and capture. Dot.cons. Dot.cons included players who teamed up with other players, consultants, or

Web site owners to commit fraud, theft, and money laundering (i.e., outside colluders); gambling insiders who provided and/or used privileged information for illegal purposes (i.e., criminal insiders); and digital teams who used bots to launder money through gambling sites (i.e., botnet herders). The typical form of organization for dot.con teams were flexible groups consisting of 2-6 associates that participated in particular criminal events in which each person had specialized roles to play. Unlike cybernomads; however, there was an elementary leadership feature as well as a principle for dividing profits. Dot.cons approached cybercrime as a working trade and developed routines for taking money from a large number of victims. Detection and arrest followed only a small fraction of the crimes committed. Assemblages. Assemblages included rings of people who distributed denial of service attacks (i.e., cyberextortion rings), those who used gambling sites to conduct identity scams on a greater scale than dot.cons (i.e., phishers), and people who worked with Internet gambling sites to further other criminal pursuits involving stealing money (i.e., money laundering). Criminal assemblages were more formal and continuous in operation than other kinds of online criminal organization. They were more sophisticated, had the most elaborate division of labour for engaging in criminal behaviour, and lasted for an extended duration across time and space. Criminal assemblages relied upon long firm fraud (i.e., 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). As larger amounts of money were being stolen in an increasingly visible way, gambling providers, regulators, police, and private security companies stepped up their efforts to prevent it. As a result, assemblages had to be prepared to take greater chances while simultaneously upgrading their techniques and planning to minimize the higher risks.

CONCLUSIONS

There are different levels of criminal organization in Internet gambling which are distinguished by the 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. Users, providers, and architects of online gambling sites have reason to be concerned 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, and a vehicle and support for crime.

KEYWORDS: crime, Internet gambling

URL: <http://jgi.camh.net/doi/abs/10.4309/jgi.2010.24.5>

Filename: Online crime and internet gambling.docx
Directory: S:\Knowledge Repository\Synopsis\Synopsis-
pdf_conversions_2017\Needs Citation
Template: C:\Users\krystal\AppData\Roaming\Microsoft\Templates\Normal.
dotm
Title:
Subject:
Author: Joseph Grady
Keywords:
Comments:
Creation Date: 2017-03-09 9:34:00 AM
Change Number: 3
Last Saved On: 2017-03-10 2:17:00 PM
Last Saved By: Krystal Luscombe
Total Editing Time: 0 Minutes
Last Printed On: 2017-03-10 2:17:00 PM
As of Last Complete Printing
Number of Pages: 2
Number of Words: 687 (approx.)
Number of Characters: 4,081 (approx.)