100% sure bets? Exploring the precipitation-control strategies of fixed-match informing websites and the environmental features of their networks

Asier Moneva[a]* and Stefano Caneppele[b]

[a]*Crímina Research Centre, Miguel Hernandez University, Elche, Spain;* [b]*Ecole des Sciences criminelles, University of Lausanne, Lausanne, Switzerland*

Correspondence: Avda. de la Universidad, s/n. Hélike building. 03201, Elche (Spain).
Email: amoneva@crimina.es

100% sure bets? Exploring the precipitation-control strategies of fixed-match informing websites and the environmental features of their networks

In recent years, many human activities have made cyberspace their preferred environment. This study focuses on the betting environment, specifically on fixed-match informing websites (FMIWs). These sites claim to be capable of selling tips about fixed sports events. They essentially act as vendors of confidential sources, allowing punters to place 100% sure bets. We hypothesize that cyber places for match-fixing tips facilitate deviant behaviours. Through systematic observation, we describe and quantify a set of 15 environmental features they share, which do not always belong to regulated online betting platforms. Findings from 78 FMIWs corroborate our hypothesis, as they support the relevance of Environmental Criminology theories applied to cybercrime. Additional exploration through hyperlink network analysis shows that FMIWs are highly homogeneous and have similar characteristics to the Tor network but differ from other illicit online environments such as sexual child exploitation networks or white supremacist communities. The characteristics of the network suggest that the business is more similar to a fraud scheme than an illicit market. Finally, the practical implications of the results for crime prevention and the directions for future research are outlined.

Keywords: fixed-match informing websites, sport betting, cyber place, situational precipitators of crime, hyperlink network analysis

Introduction

In recent years, many illicit activities (e.g., fraud, child pornography, harassment) have made cyberspace their preferred environment (Holt & Bossler, 2014). Solo offenders, criminal networks, and other groups move to online environments because of new criminal opportunities (Morselli & Décary-Hétu, 2013). These actors use cyber environments to commit crimes, organize their illicit activities, establish new links with other networks, and recruit new members, thereby facilitating the diversification of their criminal activities from, for example, traditional fraud to phishing (Leukfeldt, Kleemans, & Stol, 2017b). For criminals, online fraud is among the most prevalent and beneficial types of cybercrimes and does not require sophisticated skills beyond the motivation for

financial gain (Cross & Blackshaw, 2015). Indeed, financial gain is one of the reasons why criminal networks still incorporate low-tech all-round to high-tech specialists (Leukfeldt, Kleemans, & Stol, 2017a). The few requirements for committing crimes in cyberspace in terms of both skill and resources, together with the new criminal opportunities generated by the accessibility to this space, favour the emergence of new forms of online frauds together with online fraud markets. By fraud markets, we refer to markets through which people sell counterfeit goods (e.g., fake passports), stolen data (e.g., carding) or services (e.g., tutorials, botnets, confidential information) to facilitate further fraud. Fixed-match informing websites (FMIWs) belong to this category of markets.

In this study, FMIWs are cyber places where users buy and sell information on alleged fixed sports results. Potential users include sport-betting punters who want to place their money on fixed matches for the highest return on their investment—minimizing the risk—. An alleged market of fixed results, if false, can turn users into defrauded victims and, if true, can fuel corruption in sports. This phenomenon may be enrolled under the larger issue related to match-fixing and sports betting. Match-fixing affairs are not new in sports (Huggins, 2018), but their relevance has grown since the 2000s. Online betting boosted opportunities to place sports bets from around the world on many types of disciplines and competitions. As the size and complexity of the betting market increase, so do the size of opportunities to make money illegally (Forrest, 2012). One fraudulent way deals with adjusting sports results and earning money on sure bets. Although match-fixing is not always related to betting, the betting-related dimension of match manipulation is a crucial concern among sports federations (Moriconi & Almeida, 2019). There are two main reasons for this concern. First, sports betting is now an essential source of revenue for many disciplines, and match-fixing scandals may hamper it (Tak, 2018). Second, as suggested by the Interpol Match-Fixing Task Force, the prospect of big profits with minimal cost—in terms of risk—has led criminals to seek profit opportunities in this area[1] with negative consequences for the sport movement.

By recording recent trends in this matter, the Sports Betting Integrity (ESSA) entity reported growing numbers of match-fixing incidents to competent authorities since

[1] https://www.interpol.int/Crimes/Corruption/Corruption-in-sport

2015[2], mainly related to tennis and football (ESSA, 2015; ESSA, 2016; ESSA, 2017; ESSA, 2018). FMIWs claim to possess insider information about the outcome of a fixed match that is then fraudulently sold online. This service can be sold via the darknet and the clear web. Some recent indications point to the existence of illegal online betting platforms and darknet forums, where the results of fixed matches are marketed (CK Consulting & Stichting VU-VUmc, 2017). Additionally, taking advantage of the easy dissemination of content in the clear web, and claiming to have privileged information about these fixed matches, some websites also advertise the sale of related information on results, hoping to seduce potential buyers. Although observing the websites promoting such activities cannot confirm whether they actually possess the information they claim, what is quite evident is that, in one way or another, they are promoting fraudulent illegal activities.

Assuming postulates of environmental criminology theories are also valid in cyberspace, in this study, we aim to understand which elements of the FMIWs favour the onset of specific criminal opportunities. In particular, we use situational precipitators of crime to examine the extent to which these websites encourage users who visit them to engage in deviant behaviour. This study contributes to the literature by applying an analytical framework to the problem of FMIWs to identify their unique environmental features that facilitate their detection. We also explore the URLs contained in these websites to explore their network of connections, thereby facilitating a better understanding of their organization. We employ a network analysis technique that allows us to reveal other cyber places that comprise this network while identifying the primary nodes in this structure. We show a method for disrupting such networks that can be employed by law enforcement agencies.

Places in cyberspace: An opportunity-precipitation framework

According to environmental criminologists, the place where a crime occurs is the key organizing feature for crime analysis (Weisburd et al., 2016). However, in a review of the book, Place Matters: Criminology for the Twenty-First Century (Weisburd et al., 2016), Clarke (Clarke, 2018) argues that, for crimes committed in cyberspace, as well as some

[2] ESSA reported 100 incidents in 2015, 130 in 2016, 266 in 2017, and 267 in 2018.

types of fraud, the role of geographic location is hardly relevant. Instead, the important issue is the convergence of an offender with an environment of opportunity, which does not necessarily have to be geographical. When a motivated offender takes advantage of such opportunities in cyberspace to commit crimes, we refer to those digital convergence settings as cyber places (Miró-Llinares & Johnson, 2018).

Similar to physical places, there are different types of cyber places whose characteristics favour or hinder the concentration of specific crimes within them. While in cyber places, such as social media—where personal interaction is more frequent—one can expect a substantial incidence of social cybercrimes such as harassment, sexting, or hate speech. Cyber places devoted to consumer activities, such as shopping or banking, will host a different criminal phenomenology that is more financial. For example, some research reports that older students who spend more time in chatrooms, and younger adults who frequently use social media, are more likely to experience online harassment victimization (Marcum, Higgins, & Ricketts, 2010; Näsi, Räsänen, Kaakinen, Keipi, & Oksanen, 2017). Additionally, individuals who perform online activities like banking or shopping are more likely to experience identity theft (Reyns, 2013) or be defrauded (van Wilsem, 2013). There are two main interconnected reasons for these findings. First, the configuration of cyber places shapes the range of actions available to their users. Second, the type of activity carried out by users in an online environment affects the criminal opportunities that proliferate there. As for consumption platforms dedicated to selling products or offering services (e.g., eBay, Amazon), their configuration permits certain actions for e-commerce, and the opportunities derived from such activities make them particularly attractive for committing financially motivated cybercrimes.

Cyber places, such as websites that claim to sell results of fixed matches, can be particularly attractive for potential buyers in terms of costs versus benefits. How administrators of these websites advertise the feasibility of profiting from such activity can lead users to buy their services. Without any proper crime control websites, offering fixed matches can quickly become crime attractors. Such places are appealing to offenders because they offer particularly attractive criminal opportunities in terms of cost-effectiveness (Brantingham & Brantingham, 1995). Additionally, FMIWs' configurations are such that the mere act of visiting them constitutes a tempting situation to buy the products they offer.

According to Wortley (Wortley, 1997), there are certain situations that prompt or provoke individuals to engage in criminal behaviour. Some of the features on these

websites are situational precipitators of crime and, therefore, the Precipitation-Control Strategies established by Wortley (2001) (See Table 1), can be used classify specific strategies for avoiding them. Following the opportunity-precipitation model (Wortley, 2001), crime may be preventable by (a) avoiding precipitating criminal behaviour initially and (b) reducing opportunities to commit the crime in a subsequent stage. This model operates within Situational Crime Prevention (SCP) strategies—a set of practical measures proven highly effective in reducing crime in particular contexts (Clarke, 1997). Beyond the SCP measures that have been implemented in physical spaces, the foundations on which strategies are built have proven sufficiently robust to develop applications for online environments (Newman & Clarke, 2003). SCP models have been used to approach problems in online stolen data markets (Hutchings & Holt, 2017), develop preventive strategies for e-commerce crime (Newman & Clarke, 2003), reduce information security vulnerabilities (Hinduja & Kooi, 2013), and examine DDoS operators (Hutchings & Clayton, 2016). Overall, the literature shows that the adaptability of such strategies to new phenomena is as great as researchers' can imagine, although there is little evidence of the results of their application to crimes committed in cyberspace.

Table 1. Classification of precipitation-control strategies

Controlling Prompts	Controlling Pressures	Reducing Permissibility	Reducing Provocations
Controlling triggers	Reducing inappropriate conformity	Rule setting	Reducing frustration
Providing reminders	Reducing inappropriate obedience	Clarifying responsibility	Reducing crowding
Reducing inappropriate imitation	Encouraging compliance	Clarifying consequences	Respecting territory
Setting positive expectations	Reducing Anonymity	Personalizing victims	Controlling environmental irritants

Source: Adapted from Wortley (2001)

Aims of the study

The analysis of FMIWs has received little attention in academia. Most of the research addresses the broader topic of match-fixing in international sports (Haberfeld & Sheehan, 2013). Aiming to fill this gap in the literature, this paper focuses on (alleged) FMIWs and

their networks. Adopting Wortley's (2001) Precipitation-Control Strategies framework, we hypothesize the following:

H1. FMIWs offer specific crime opportunities because they incorporate distinctive environmental features that incentivize deviant behaviours (i.e. buying fixed matches results) when compared to regulated sport-betting websites.

H2. Due to the peculiarity of this cyber environment, vending places for fixed matches have a specific network compared to a random network distribution.

Method

Sampling: Detection and selection of the websites

This study follows a methodology similar to that proposed by Pineau et al. (2016) to obtain a sample of websites from the clear web related to fixed matches. After defining a list of keywords[3], they were entered into the Tor browser using the DuckDuckGo search engine, a strategy followed to improve anonymity. Then, the first 50 results for each keyword were manually checked (i.e. 200 URLs visited) to determine whether these websites offer information in exchange for money about supposedly fixed matches. Through this process, 78 websites that met the inclusion requirements were identified as an FMIW (Appendix A Table 5). To determine the extent to which the characteristics that define FMIWs as crime attractors differ from other cyber places, a second set of websites was selected for comparison purposes. The authors considered a list of 28 regulated sport-betting sites (Appendix B Table 6). To ensure that this second group of websites had a legitimate origin, we referred to the list of members belonging to two official international entities that promote integrity in betting: The World Lottery Association (WLA), and ESSA.

Analytic strategy

Two analysis techniques were used to achieve the established objectives set, including

[3] (1) match-fixing, (2) fixed betting tips, (3) fixed matches, (4) fixed-odd sports.

(1) systematic observation, to detect the situational features of the websites and (2) network analysis, to describe the structure of fixed matches vending cyber-places.

Systematic observation

Systematic observation in the social sciences is based on the identification of a series of items in a specific context whose presence or absence can be objectively determined (Mastrofski, Parks, & McCluskey, 2010; Reiss, 1971). For example, this methodology has been used to quantify the social and physical properties of neighbourhoods such as urban disorder (Raudenbush & Sampson, 1999; Sampson & Raudenbush, 1999), or to study police work in public settings (Mastrofski et al., 1998).

This study proposes a modality of systematic observation to compare cyber places that allows for quantifying the situational features that configure them. Through an observational process, we first identified 15 items that usually define the environmental design of sport-betting websites. Next, we adapted and classified each item as a technique under precipitation-control strategies (Wortley, 2001). The systematic observation was conducted on two subsets: (1) FMIWs and (2) regulated sport-betting websites. After recording the elements observed on both illicit and regulated web pages, we compared the results to determine which of these cyber places incorporate more techniques that regulate behaviours of the users who visit them. In theory, the subset of websites that incorporates fewer of these features in its design will have less control over the behaviour of its users, a circumstance that may turn them into crime attractors. On the contrary, a greater presence of features appears on regulated websites. Table 2 shows a description of the items that were observed and subsequently checked for each of the sampled websites.

Table 2. Situational precipitators, and specific observed items on sport-betting websites with a description

Situational precipitator typologies by item	Description
Controlling prompts	
Controlling triggers	
Advertisements of other betting sites	The website does not incorporate a banner linked to an external betting site.
Providing reminders	
Self-restriction measures	The website facilitates tools or utilities for users to limit their betting.
Advice on abusive gaming	The website provides tips for detecting signs of or resources for mitigating abusive gambling.
Setting positive expectations	
Operator and contact information	The website exhibits legal information of the site operator as well as visible contact channels.
License number/model	The website displays a license model or number authorizing the activity.
Privacy and cookies policy	The website has a privacy policy that includes a cookie policy.
Controlling pressures	
Reducing anonymity	
Registration/login system	The website integrates a user login system for accessing its services.
Reducing permissibility	
Rule setting	
Required payment methods	The website specifies which payment systems are allowed.
Terms and conditions of use	The website has a guideline of terms and conditions of use of its services.
Protection of minors	The website has a policy of restricting access to minors.
Clarifying consequences	
Copyright information	The website shows the copyright information of its domain.
Reducing provocations	
Reducing frustration	
Help/FAQ section	The website contains a user help section or frequently asked questions.
Site language options	The website allows the user to change the language in which its contents are communicated.
Controlling environmental irritants	
Menu	The website has a menu that facilitates navigation.
Smooth, responsive interface	The website has a pleasant and functional interface that makes navigation enjoyable.

Hyperlink network analysis

The second objective of the research was to survey the network structure among the sampled FMIWs. We used hyperlink network analysis (HNA) to review the linked

websites (Park, 2003; Park & Thelwall, 2006; Thelwall, 2004). HNA focuses on relationships among websites and recalls the same techniques and metrics used by social network analysis, which focuses on social relationships. For example, researchers have used HNA to explore the structure of online child sexual exploitation networks in a criminological context (Westlake & Bouchard, 2016), as well as to examine the structure of white supremacist online communities in a sociological one (Burris, Smith, & Strahm, 2000).

To collect data on websites' relationships, we implemented the use of a web crawler that allows data scraping with the R software using the RCrawler package (Khalil & Fakir, 2017). This package offers a function that facilitates the retrieval of external links from a given website and their storage in a data frame with an appropriate structure (i.e., which websites the links come from and to where they are directed) to apply network analysis (Wasserman & Faust, 1994). We then pre-processed the stored URLs to identify unique domains. This process enabled the creation of a targeted network wherein the nodes are websites, and the edges are their connections, represented by a linking URL. In all, 923 unique cyber places were identified within the network with 2306 links between them. We then calculated several standard network metrics, including density, reciprocity, diameter, and mean distance. We compared the obtained results with those of 1000 simulated networks that share the same characteristics as the observed one (i.e., direction, density, number of nodes, and number of edges). All network analyses were performed with the Igraph package in R (Csárdi & Nepusz, 2006).

Ethical issues

Results appear in aggregate format and omit any information that could lead to the individualization of users. However, the researchers cannot assume responsibility if this type of information is publicly available by website administrators on some of the websites that appear listed in Appendix A Table 5.

Results

Comparison between regulated sport-betting websites and illicit FMIWs

Table 3 shows the different characteristics observed between legitimate cyber places and those supposedly selling fixed-match results. The results indicate that all precipitation-

control techniques manifest themselves more often on regulated websites than they do on FMIWs (χ^2 (14, $N = 15$) = 400.54, $p < .001$). Further, 9 of 15 techniques appear on all regulated websites, and the other six appear in more than 50% of cases. Three techniques never appear on FMIWs, and seven additional techniques are present less than 10% of the time.

Table 3. Differential presence of precipitation-control strategies by type of cyber place

Precipitation-control strategies and techniques	Regulated websites (*n* = 28)		FMIWs (*n* = 76)	
	n	%	n	%
Controlling prompts				
Controlling triggers				
Avoid other betting sites advertisements	28	100.0	4	5.3
Providing reminders				
Facilitate self-restriction measures	23	82.1	0	0.0
Advise on abusive gaming	28	100.0	2	2.7
Setting positive expectations				
Exhibit operator and contact information	28	100.0	1	1.3
Display a license number/model	19	67.9	0	0.0
Have a privacy and cookies policy	28	100.0	5	6.7
Controlling pressures				
Reducing anonymity				
Enable registration/login	28	100.0	0	0.0
Reducing permissibility				
Rule setting				
Set payment methods	17	60.7	37	49.3
Establish terms and conditions of use	27	96.4	8	10.7
Discourage the participation of minors	28	100.0	5	6.7
Clarifying consequences				
Show copyright information	19	67.9	44	58.7
Reducing provocations				
Reducing frustration				
Provide help/FAQ	28	100.0	9	12.0
Enable site language options	15	53.6	1	1.3
Controlling environmental irritants				
Embed a menu	28	100.0	57	76.0
Design a smooth responsive interface	28	100.0	2	2.7

There are vast differences in almost all the techniques described. A paradigmatic example is the technique aimed at controlling triggers (e.g., avoid other betting sites' advertisements), which always appear on regulated websites, but only in 5.3% of fixed matches ones. The remaining illicit websites embed advertising banners that redirect users to other fixed matches domains, thereby forming a network of websites.

Analysis of the FMIW network

After visiting each of the FMIWs that compose the nodes of the network, we assigned them an additional attribute that indicates the type of cyber place they are. These assigned attributes indicate whether each site is one of the following: (1) sites that trade fixed match results; (2) regulated sport-betting sites; (3) social media sites; (4) platforms that offer web services or utilities; (5) online payment systems; and (6) other cyber places. The last category includes websites that did not belong to any of the previous categories, as well as links that were outdated, broken, expired, or redirected to different websites. The distribution of nodes, according to the type of cyber place they are, appears in Table 4. When examining the nodes of the network, besides those categorized as fixed match sites, some websites and web applications commonly accessed by Internet users were found. For example, the crawler captured regulated betting sites such as William Hill, Bet365, and 188bet (Appendix C Table 7); web services, including WordPress, SurveyMonkey, and Imgur; social media sites like WhatsApp, Instagram, Facebook, Twitter, and YouTube; payment systems like Western Union, PayPal, Bitcoin, MoneyGram, Skrill and Neteller; and other websites, such as the Gmail email system, the top Spanish football competition LaLiga, the European law enforcement agency Europol, Wikipedia, the iTunes platform, and the Daily Mail newspaper. Although it has undoubtedly been detected that these nodes belong to the observed network, their inclusion does not imply that they do so willingly; instead, they were likely hyperlinked without their consent to some of the FMIWs.

Table 4. Network composition by type of node

Type of node	Composition (n = 923)	
	n	%
FMIW	715	77.5
Regulated betting site	26	2.8
Web service	14	1.5
Social media	7	0.8
Payment system	7	0.8
Other	154	16.7

An initial scan of FMIWs shows that they tend to include advertisements of other similar sites, suggesting that they may be connected. Of the 78 websites initially sampled, all are interconnected except two, causing the resulting network to consist of a large graph

made up of 866 nodes, a small graph comprising 55 nodes, and a micrograph of 2 (Figure 1). To examine the entire network's cohesiveness, we calculated its density, which measures the ratio of observed edges to the number of possible edges. Our network has a density of 0.003 (0.3%), indicating that its nodes are poorly connected.

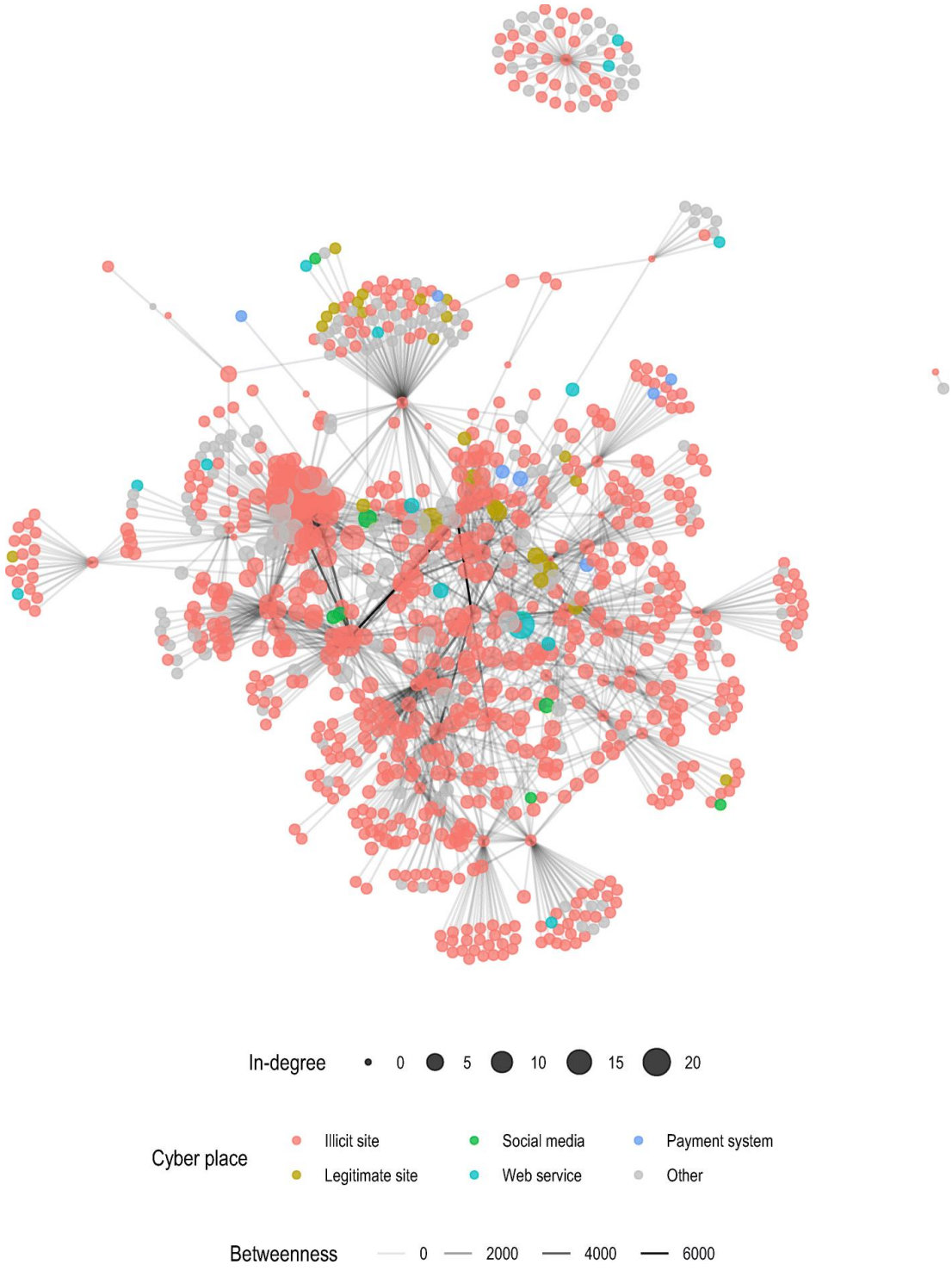

Figure 1. Network of FMIW. All figures illustrating this manuscript have been created using the ggplot2 R package (Wickham, 2016).

We then calculated three additional metrics that help to describe the network further. These metrics included (1) reciprocity, which accounts for the proportion of bidirectional links between nodes; (2) diameter, which measures the size of the network by calculating the length of the longest observed geodesic distance; and (3) mean distance, which represents the mean length of all the shortest paths leading to or coming from each vertex. We compared the obtained results with those of 1000 simulated networks that share the same characteristics as the observed one (i.e., direction, density, number of nodes, and number of edges). The observed network presents a reciprocity of 0.09 (9.1%), a diameter of 11, and a mean distance of 4. Compared to simulated networks, these results show that the observed reciprocity is notably larger than expected, whereas the diameter and mean distance are about half of the expected values (Figure 2).

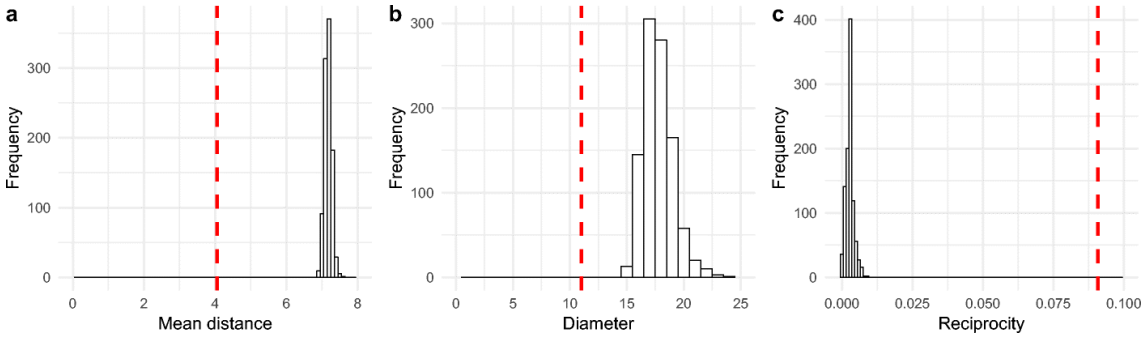

Figure 2. Comparison between metrics of the network observed and 1000 simulated. The dashed red line indicates the values obtained for the FMIW network

At the vector level, we calculated two centrality measures to identify the most salient nodes in terms of accessibility within the network, including in-degree and edge betweenness. In-degree measures the number of adjacent nodes terminating at them, an indicator of the ease with which a given website can be accessed from another. The distribution of the in-degree score by network nodes appears in Figure 3. The average in-degree score of the observed network is 2.49, indicating that most nodes receive few hyperlinks. When a node has a high in-degree score, it is referred to as a receiver node (Wasserman & Faust, 1994). Such nodes are represented with a larger size in the network, as depicted in Figure 1. Edge betweenness measures the number of shorter paths that pass through an edge connecting the key nodes or bridges that are critical for the connectivity of a network (Wasserman & Faust, 1994). In Figure 1, bridges are represented by more

opaque lines connecting their nodes; only a few nodes are connected by edges with high betweenness.

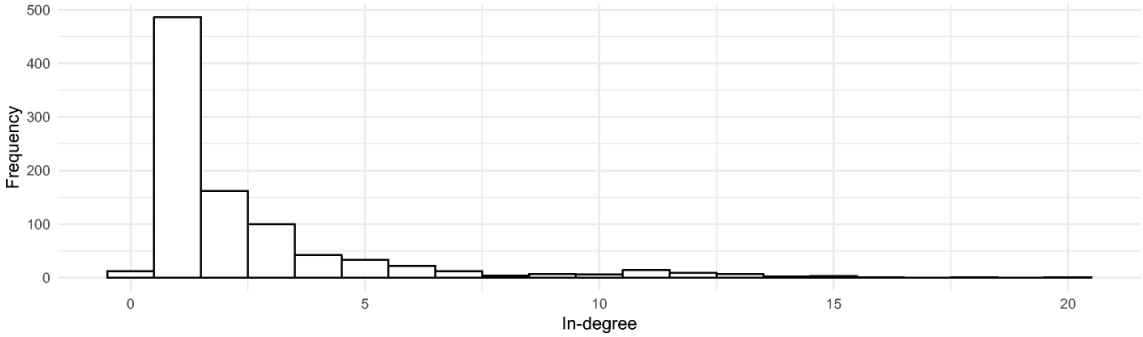

Figure 3. Network in-degree score distribution (min = 0; Mdn = 1; M = 2.49; SD = 2.73; max = 20)

Discussion

This study applied the concepts of environmental criminology to cyber places and, in particular, to FMIWs. These websites, which claim to sell tips on fixed sporting events, were mostly available on the clear web and may be crime attractors because they offer particularly attractive criminal opportunities. We hypothesized that these websites offered distinctive environmental features to incentivize deviant behaviours (buying fixed matches results) compared to regulated sport-betting websites. The results appear to corroborate our hypothesis. In general, FMIWs abound of situational precipitators. They promote triggers by posting advertisements on other betting/fixed match sites; however, they do not provide reminders to discourage pathological gambling, nor they do control prompts displaying contact information or license number (even fakes ones). Additionally, they encourage anonymity without enabling registration and login.

The contrasts are stark compared to regulated sport-betting operators' websites, which usually must comply with established guidelines and regulations. Compliance with regulatory standards facilitates a certain homogeneity in terms of reducing situational precipitators. For example, all regulated sport-betting operators discourage the participation of minors, give advice on abusive gaming, and require registration/login to play. Still, including a banner with an external link to another website has a clear, intentional nature and is not a common practice on regulated betting websites. This component of purposiveness has been evidenced by the existing literature on hyperlinked websites (Park & Thelwall, 2006). Eventually, FMIWs present distinctive layout signs,

which facilitate the precipitation to deviant conducts (in our case to buy illegal tips). Our study does not discuss how much this approach is successful in terms of business, but argues that all FMIWs share a pattern with similar environmental features that characterize them as cyber places which are "located" in the sport-betting cyber environment (Miró-Llinares & Johnson, 2018).

In the present study, we also hypothesized that vending places for fixed matches have a specific network compared to a random network distribution. The results of the study corroborate this second hypothesis as well. The network structure of FMIWs reveals more about the nature of these cyber places. First, the network is highly homogeneous. The majority of nodes (77.4%) are fixed-match sites. Previous studies on hyperlinked networks in political contexts show that they generally form homogeneous communities (Ackland & Shorish, 2009; Burris et al., 2000). The same trend appears in the match-fixing network, which is comprised of 77.4% illicit betting cyber places. However, this trend has not been observed in online child sexual exploitation communities (Westlake & Bouchard, 2016). Compared to traditional criminal networks, studied by Malm and colleagues (Malm, Bichler, & Van De Walle, 2010), the density of the observed network—0.003—resembles that of a kinship or formal organization networks—0.004 for both—rather than co-offending or legitimate associates. The former networks are characterized as being more cohesive and, thus, not easily disrupted. However, the figures for average and maximum in-degree centrality in the observed network—2.49 and 20, respectively—appear most similar to those of co-offending networks described by Malm et al. (2010). Therefore, it appears that fixed matches website network cannot be included in any of the four categories established by Malm et al., which makes it more reasonable to compare their characteristics with hyperlinked networks instead of social networks.

Hyperlinked networks, such as Tor, show values similar to the observed network—0.002 (Monk, Mitchell, Frank, & Davies, 2018). Conversely, other hyperlinked networks, such as child sexual exploitation websites, show a much higher density—an average of 0.45 for sites and 0.34 for blogs (Westlake & Bouchard, 2016); white supremacist communities have a density of 0.11 (Burris et al., 2000). Despite showing a high level of reciprocity with regard to simulated networks, as well as the Tor network (4.9%) (Monk et al., 2018), the reciprocity of the match-fixing network is small (9.1%) when compared to the online child sexual exploitation websites network (23%) (Westlake & Bouchard, 2016). Regarding network connectivity, the average distance of

the observed network, 4, is also lower when compared to Tor, which is 4.95 (Monk et al., 2018), meaning that it takes about one less connection on average to move from one node to another. Compared to child sexual exploitation, the analysed network of FMIWs has different characteristics. Specifically, the distance between its nodes is shorter, its connectivity is lower, it lacks communitarian places like forums, and it sells allegedly fixed-match results. Therefore, the network structure should be more similar to network marketplaces.

The characteristics of the network show similarities to those of the Tor network, a network that hosts these marketplaces and favours the anonymity of its users. Still, it is debatable whether FMIWs are an actual illicit market instead of a scam business model. Indeed, there are several points that support the scam hypothesis. Structurally, the alleged fixed matches market does not provide any warranty (such as escrow schemes) to protect buyers from frauds. An escrow system would reinforce trust toward vendors, and it could expand the market. Economically, the business model of selling tips on fixed matches looks weak. Once the information on fixed matches is sold, and many punters bet on the fixed match, the odds will be lowered by betting algorithms. Additionally, it is questionable why a group with insider information would sell tips on fixed matches instead of only using this information internally. The internal use would minimize the risk that fixed matches would be highlighted as suspicious, which may trigger investigations from sports federations or law enforcement. Finally, using the information to place bets on fixed matches, either directly or through a group, may generate significant rewards that the dissemination of confidential information would hamper.

Conclusion

This study focused on FMIWs and their networks. Through the concepts of cyber places and Wortley's situational precipitators framework, we corroborated the hypothesis that online match-fixing services share a typical pattern in layout design, and that they form a specific cyberenvironment: a niche market where users trade fixed-match information. Our descriptive analysis showed that FMIWs starkly differ from other regulated sport-betting websites and that they are conceived to limit environmental inhibitors and to facilitate deviant behaviours, pushing potential punters to buy fixed-match tips. The HNA provided further insight into this structure. FMIWs form a quite homogeneous environment, they have a lower density, and higher reciprocity compared to similar

random networks, but lower compared to other online illicit communities (e.g., child pornography, white supremacist). From a practical point of view, in terms of prevention, it would be interesting to apply the concept of 'secured by design' to cyber places adopting some situational crime prevention measures to avoid crime victimization (Davey, Wootton, & Wootton, 2017). Further, in terms of investigation and repression, law enforcement could use the HNA to highlights those websites that have a higher betweenness centrality. Targeting bridges should be particularly useful in reducing the robustness of the network (Malm & Bichler, 2011; Malm et al., 2010). Targeting nodes with bridging ties could facilitate policing efforts to disrupt networks (McGloin, 2005).

Nevertheless, our research has limitations. We conducted the initial sampling by using keywords, so a new search that includes additional or different words may reveal new fixed-match networks not analysed in this study. Since the search used language with Western letters, our results do not automatically extend to FMIWs in other languages that use different typing characters, whether they exist (e.g., the most spoken languages in the Asian market where sports betting is very important). In analysing the network, it was sometimes difficult to classify web pages within the proposed categories of cyber places.

Further research on different stages may also be useful. Such research should explore the applicability of secured by design principles to cyber places and, through HNA, corroborate whether and why cybercrime places have similar or different network structures, as well as explore the network survivability. Regarding FMIWs, further contributions could compare the business model used by different fixed-match vendors (e.g., prices, warranty, payment methods, types of bets sold), their prediction accuracy and the types of sport matches allegedly fixed and, eventually, establishing contact with vendors to understand how they manage the relationship with customers and the extent to which such vendors are fraudulent. Research could also explore FMIW administrator motivations to determine whether they seek personal profit as a way of promoting illegal betting. Finally, it would be interesting to understand how the punters perceive these sites and how they use them.

Acknowledgements

This work was funded by the Spanish Ministry of Science, Innovation and Universities under Grant FPU16/01671.

This is a post-peer-review, pre-copyedit version of an article published in Crime, Law and Social Change. The final authenticated version is available online at: https://doi.org/10.1007/s10611-019-09871-4.

References

Ackland, R., & Shorish, J. (2009). Network Formation in the Political Blogosphere: An Application of Agent Based Simulation and e-Research Tools. *Computational Economics*, *34*(4), 383–398. https://doi.org/10.1007/s10614-009-9173-7

Brantingham, P. L., & Brantingham, P. L. (1995). Criminality of place: Crime generators and crime attractors. *European Journal on Criminal Policy and Research*, *3*(3), 5–26. https://doi.org/10.1007/BF02242925

Burris, V., Smith, E., & Strahm, A. (2000). White Supremacist Networks on the Internet. *Sociological Focus*, *33*(2), 215–235. https://doi.org/10.1080/00380237.2000.10571166

CK Consulting & Stichting VU-VUmc. (2017). *The monitoring systems of sports betting and warning mechanisms between public and private actors* (pp. 1–245). Retrieved from http://ethisport.com/wp-content/uploads/sites/28/2017/06/Betmonitalert_Design-NB-DEF-2-06-2017.pdf

Clarke, R. V. (Ed.). (1997). *Situational crime prevention: Successful case studies* (2. ed). Guilderland, NY: Harrow and Heston.

Clarke, R. V. (2018). Book Review. *Journal of Criminal Justice Education*, *29*(1), 157–159. https://doi.org/10.1080/10511253.2016.1258031

Cross, C., & Blackshaw, D. (2015). Improving the Police Response to Online Fraud. *Policing*, *9*(2), 119–128. https://doi.org/10.1093/police/pau044

Csárdi, G., & Nepusz, T. (2006). The igraph software package for complex network research. *InterJournal, Complex Systems*, *1695*(5), 1–9.

Davey, C. L., Wootton, A. B., & Wootton, A. B. (2017). *Design Against Crime: A Human-Centred Approach to Designing for Safety and Security*. https://doi.org/10.4324/9781315576565

ESSA. (2015). *ESSA Q4 2015 Integrity Report* (pp. 1–6). Retrieved from http://www.eu-ssa.org/wp-content/uploads/QR4-BROCHURE-WEB.pdf

ESSA. (2016). *ESSA 2016 Annual Integrity Report* (pp. 1–6). Retrieved from http://www.eu-ssa.org/wp-content/uploads/QR1-BROCHURE-2017-SINGLE.pdf

ESSA. (2017). *ESSA 2017 Annual Integrity Report* (pp. 1–6). Retrieved from http://www.eu-ssa.org/wp-content/uploads/ESSA-2017-annual-integrity-report.pdf

ESSA. (2018). *ESSA 2018 Annual Integrity Report* (pp. 1–6). Retrieved from http://www.eu-ssa.org/wp-content/uploads/ESSA-2018-Annual-Integrity-Report.pdf

Forrest, D. (2012). The Threat to Football from Betting-Related Corruption. *International Journal of Sport Finance*, *7*(2), 99–116.

Haberfeld, M. R., & Sheehan, D. (Eds.). (2013). *Match-Fixing in International Sports*. https://doi.org/10.1007/978-3-319-02582-7

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, *26*(4), 383–402. https://doi.org/10.1057/sj.2013.25

Holt, T. J., & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Huggins, M. (2018). Match-Fixing: A Historical Perspective. *The International Journal of the History of Sport*, *35*(2–3), 123–140. https://doi.org/10.1080/09523367.2018.1476341

Hutchings, A., & Clayton, R. (2016). Exploring the Provision of Online Booter Services. *Deviant Behavior*, *37*(10), 1163–1178. https://doi.org/10.1080/01639625.2016.1169829

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime*, *18*(1), 11–30. https://doi.org/10.1080/17440572.2016.1197123

Khalil, S., & Fakir, M. (2017). RCrawler: An R package for parallel web crawling and scraping. *SoftwareX*, *6*, 98–106. https://doi.org/10.1016/j.softx.2017.04.004

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, *67*(1), 21–37. https://doi.org/10.1007/s10611-016-9662-2

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks. *British Journal of Criminology*, *57*(3), 704–722. https://doi.org/10.1093/bjc/azw009

Malm, A., & Bichler, G. (2011). Networks of Collaborating Criminals: Assessing the Structural Vulnerability of Drug Markets. *Journal of Research in Crime and Delinquency*, *48*(2), 271–297. https://doi.org/10.1177/0022427810391535

Malm, A., Bichler, G., & Van De Walle, S. (2010). Comparing the ties that bind criminal networks: Is blood thicker than water? *Security Journal*, *23*(1), 52–74. https://doi.org/10.1057/sj.2009.18

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behavior*, *31*(5), 381–410. https://doi.org/10.1080/01639620903004903

Mastrofski, S. D., Parks, R. B., & McCluskey, J. D. (2010). Systematic Social Observation in Criminology. In A. R. Piquero & D. Weisburd (Eds.), *Handbook of Quantitative Criminology* (pp. 225–247). https://doi.org/10.1007/978-0-387-77650-7_12

Mastrofski, S. D., Parks, R. B., Reiss, A. J., Worden, R. E., De Jong, C., Snipes, J. B., & Terrill, W. (1998). *Systematic social observation of public police: Applying field research methods to policy issues.* [Research Report]. Retrieved from National Institute of Justice website: https://www.ncjrs.gov/pdffiles/172859.pdf

McGloin, J. M. (2005). Policy and intervention considerations of a network analysis of street gangs. *Criminology & Public Policy*, *4*(3), 607–635. https://doi.org/10.1111/j.1745-9133.2005.00306.x

Miró-Llinares, F., & Johnson, S. D. (2018). Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace. In G. J. N. Bruinsma & S. D. Johnson (Eds.), *The Oxford Handbook of Environmental Criminology* (pp. 883–906). https://doi.org/10.1093/oxfordhb/9780190279707.013.39

Moneva, A., & Caneppele, S. (2019). 100% sure bets? Exploring the precipitation-control strategies of fixed-match informing websites and the environmental features of their networks. *Crime, Law and Social Change*, 1–19. https://doi.org/10.1007/s10611-019-09871-4

Monk, B., Mitchell, J., Frank, R., & Davies, G. (2018). Uncovering Tor: An Examination of the Network Structure. *Security and Communication Networks*, *2018*, 1–12. https://doi.org/10.1155/2018/4231326

Moriconi, M., & Almeida, J. P. (2019). Portuguese Fight Against Match-Fixing: Which Policies and What Ethic? *Journal of Global Sport Management*, *4*(1), 79–96. https://doi.org/10.1080/24704067.2018.1493357

Morselli, C., & Décary-Hétu, D. (2013). Crime facilitation purposes of social networking sites: A review and analysis of the 'cyberbanging' phenomenon. *Small Wars & Insurgencies*, *24*(1), 152–170. https://doi.org/10.1080/09592318.2013.740232

Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2017). Do routine activities help predict young adults' online harassment: A multi-nation study. *Criminology & Criminal Justice*, *17*(4), 418–432. https://doi.org/10.1177/1748895816679866

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery preventing e-commerce crime*. Milton Park: Routledge Chapman & Hall.

Park, H. W. (2003). Hyperlink network analysis: A new method for the study of social structure on the web. *Connections*, *25*(1), 49–61.

Park, H. W., & Thelwall, M. (2006). Hyperlink Analyses of the World Wide Web: A Review. *Journal of Computer-Mediated Communication*, *8*(4). https://doi.org/10.1111/j.1083-6101.2003.tb00223.x

Pineau, T., Schopfer, A., Grossrieder, L., Broséus, J., Esseiva, P., & Rossy, Q. (2016). The study of doping market: How to produce intelligence from Internet forums. *Forensic Science International*, *268*, 103–115. https://doi.org/10.1016/j.forsciint.2016.09.017

Raudenbush, S. W., & Sampson, R. J. (1999). Ecometrics: Toward a Science of Assessing Ecological Settings, with Application to the Systematic Social Observation of Neighborhoods. *Sociological Methodology*, *29*(1), 1–41. https://doi.org/10.1111/0081-1750.00059

Reiss, A. J. (1971). Systematic Observation of Natural Social Phenomena. *Sociological Methodology*, *3*, 3. https://doi.org/10.2307/270816

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238. https://doi.org/10.1177/0022427811425539

Sampson, R. J., & Raudenbush, S. W. (1999). Systematic Social Observation of Public Spaces: A New Look at Disorder in Urban Neighborhoods. *American Journal of Sociology*, *105*(3), 603–651. https://doi.org/10.1086/210356

Tak, M. (2018). Too big to jail: Match-fixing, institutional failure and the shifting of responsibility. *International Review for the Sociology of Sport*, *53*(7), 788–806. https://doi.org/10.1177/1012690216682950

Thelwall, M. (2004). *Link analysis: An information science approach*. Amsterdam: Elsevier Academic Press.

van Wilsem, J. (2013). 'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization. *European Sociological Review*, *29*(2), 168–178. https://doi.org/10.1093/esr/jcr053

Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge ; New York: Cambridge University Press.

Weisburd, D., Eck, J. E., Braga, A. A., Telep, C. W., Cave, B., Bowers, K., … Yang, S.-M. (2016). *Place Matters: Criminology for the Twenty-First Century*. https://doi.org/10.1017/CBO9781139342087

Westlake, B. G., & Bouchard, M. (2016). Liking and hyperlinking: Community detection in online child sexual exploitation networks. *Social Science Research*, *59*, 23–36. https://doi.org/10.1016/j.ssresearch.2016.04.010

Wickham, H. (2016). *ggplot2: Elegant graphics for data analysis* (Second edition). Cham: Springer.

Wortley, R. (1997). Reconsidering the role of opportunity in situational crime prevention. In G. R. Newman, R. V. Clarke, & S. G. Shoham (Eds.), *Rational Choice and Situational Crime Prevention* (pp. 65–81). Aldershot: Ashgate Publishing.

Wortley, R. (2001). A Classification of Techniques for Controlling Situational Precipitators of Crime. *Security Journal*, *14*(4), 63–82. https://doi.org/10.1057/palgrave.sj.8340098

Appendices

A. Selected illicit FMIWs by number of external URL

Table 5. Selected illicit FMIWs by number of external URL

Address	External URL
http://www.fixed-match.us/	163
https://master-fixed.com/	125
https://europol-fixed.com/	111
http://fixed-tips1x2.com/	99
https://1x2bettingtips.com/	85
https://prelazi-dojavi.com/	69
https://9ja-fixed.com/	68
http://juventus-bet.com/	64
http://williamhill1x2.com/	60
http://www.asia-fixedmatches.com/	59
http://fixed-advisor.com/	58
http://soccer-predictions.co.uk/	57
https://fixedmatchtip.com/	55
http://tips-free.com/	55
http://www.verifiedsoccertips.com/	55
https://fixedmatches.tips/	55
https://mata-fixed.tips/	51
https://bettingfixed.com/	50
https://fixedsafematches.com/	49
https://topbet-fixed.com/	48
https://america-fixedmatches.com/	48
https://fcfixedmatches.com/	47
https://fixed-matches.football/	46
https://fixedmatches.website/	46
https://fixed-matches.sportal.tips/	45
https://betting-predictions.football/	43
http://falcao1x2.com/	42
https://match-fixing.sportal.tips/	41
http://www.bestfixedmatches1x2.com/	41
http://matchesfixing.com/	38
http://betting-fixed.com/	37
http://matches-fixed.com/	37
https://manipulated-fixed-matches.sportal.tips/	36
https://www.realfixedmatches.com/	36
http://betyetu-fixed.com/	34
https://truefixedmatches1x2.com/	34
http://viti-bet.com/	33
https://www.freesupertips.co.uk/free-football-betting-tips/	33
http://fixedinsider.com/	32
http://supabet-fixed.com/	31
https://helena1x2.sportal.tips/	30
https://soccer-fixed.tips/	30
http://fixed-odd.com/	30
http://fixedmatches.uk/	28
https://adibet.tips/	27
https://fixed-matches.tips/	27
http://stat-area.com/	26
https://xanthi-fixed.matches.sportal.tips/	25
http://fixed-scores.com/	23
https://hotfixedmatches.com/	21
https://sonkotips.com/free-betting-tips/	20
http://site-fixed-matches.com/	20
https://real-fixedmatches.com/	20
https://www.qatar-fixed.com/	19

Address	External URL
https://basel-fixedmatches.com/	19
https://fixed.tips/	18
https://larsbetting.com/	14
https://fixedmatches.mobi/	13
https://www.paidpicks1x2.com/	13
https://strongfixedmatches.com/	13
https://predictz-tips.com/fixed-match/	10
https://fixedmatches-betting.com/	8
https://fixedmatches-seller.com/	8
https://fixedmatches-betting.com/	8
https://thefixedmatches.com/	7
https://www.fixed-betting-tips.com/	5
http://swiss-fixed.com/	5
https://fixedmatches.football/	5
https://matchfixed.com/	5
https://www.fixdrawsoccer.com/	3
https://fixedmatches.today/	3
https://www.oddstips.co.uk/	3
https://betting1x2.football/	2
http://fixed.matches1x2.com/	2
https://theopicks.com/fixed-matches-single/	2
http://www.fixedbetting.tips/	1
http://www.fixedodd.tips/	1
http://www.bestfootballtips.net/	1

B. Selected regulated sport-betting websites by operator

Table 6. Selected regulated sport-betting websites by operator

Address	Operator
888sport.com	Cassava Enterprises
bet365.com	Hillside (Sports) ENC
betclic.fr	BetClic Enterprises
betfred.com	Petfre
betsson.com	BML Group
betvictor.com	BetVictor
betway.com	Betway
danskespil.dk/oddset	Danske Spil
e-lotto.be	Loterie Nationale
enligne.parionssport.fdj.fr	Parions Sport En Ligne
e-stave.com	Športna loterija
fonbet.com	Leofon
interwetten.com/en/sportsbook	Interwetten Gaming
jeux.loro.ch/sports	Loterie Romande
lottomatica.it/scommesse/avvenimenti	Lottomatica
pamestoixima.gr	Pamestoixima
sisal.it	Sisal Entertainment
skybet.com	Bonne Terre
spela.svenskaspel.se/europatipset	Svenska Spel Sport & Casino AB
sportingbet.com	ElectraWorks
sportingindex.com	Sporting Index

Address	Operator
sports.williamhill.com/bet/en-gb	WHG
swisslos.ch/fr/sporttip/parissportifs/prognostics.html	Swisslos Lotería Intercantonal
tipkurz.etipos.sk	Tipos
tippmixpro.hu	Szerencsejáték Zrt
unibet.com	Trannel International
veikkaus.fi/fi/live-veto	Veikkaus
win2day.at/sportwetten	Österreichische Lotterien GmbH

C. List of regulated betting sites found in the FMIW network

Table 7. List of regulated betting sites found in the FMIW network

Address	Operator
williamhill.com	WHG
bet365.com	Hillside (Sports) ENC
188bet.com	Cube Limited
betboro.com	Webmedia Development N.V.
betvictor.com	BetVictor
bigbetworld.com	M-Hub Gaming Operations (inactive)
ladbrokes.com.au	GVC Australia
paddypower.com	PPB Counterparty Services
sbobet.com	SBOBET
12bet.com	TGP Europe
betsson.com	BML Group
betway.com	Betway
bwin.com	ElectraWorks
betfred.com	Petfre
mybet.com	Rhinoceros Operations
nordicbet.com	BML Group
odds.betsafe.com	BML Group
skybet.com	Bonne Terre
sportingbet.com	ElectraWorks
stanjames.com	Platinum Gaming
unibet.com	Trannel International
betway.com	Betway
sports.coral.co.uk	Coral Interactive
bet9ja.com	KC Gaming Networks
marathonbet.com	Marathonbet Spain
sports.ladbrokes.com	Ladbrokes Betting & Gaming