What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud

Aunshul Rege[1]
Rutgers University, USA

Abstract

Cyberspace has become an alternative medium for experiencing new and creative romantic endeavors with few spatio-temporal limits. E-love networks have proliferated since the mid-1990s and are expected to generate $1.9 billion by 2012. However, this successful global industry is a frequent venue of cyber crime, which poses serious problems for matchmaking services and daters worldwide. This paper offers an overview of romance scams and identity fraud at dating sites, developing a typology of cyber criminals and analyzing each type along the dimensions of criminal techniques, organizations, and ideologies. The theoretical framework for this paper borrows from criminal organization and network-based theories. Document analysis is conducted on data from dating sites, news and media sites, anti-scam commissions, law enforcement agencies, and government agencies, from 2000 to 2009. Twenty keyword combinations are used to gather 170 documents, which are then sorted around four intersecting themes: online dating, scams and frauds, the organization of cyber criminals, and prevention and regulation. This paper concludes that the three dimensions of technology, cyberspace, and inadequate countermeasures collectively influence criminal organization and operation in cyberspace.

Keywords: Cyber crime; Cybercriminal; Typology; Romance Scams; Identity Fraud.

Introduction

The rapid development of information and communication technologies (ICTs) and the prevalence of the internet offer an alternative venue for romantic endeavors. Internet daters experience excitement when they interact with other people through new, digital mediums. Four factors make online dating attractive to customers. First, individuals do not have to leave their homes or workplaces to date. Matchmaking sites are open for business 24 hours a day, 7 days a week, allowing daters to remotely scan profiles at their convenience. Second, the anonymity feature of the internet allows individuals to participate privately in dating without the oversight of others or the fear of stigma. Third, interactive online dating allows customers to experience new forms interaction, such as live chats, instant messaging, flirtatious emoticons, nudges, and winks (Fiore & Donath, 2004; Wang & Lu, 2007). Fourth, online dating sites serve up 'perfect matches' quickly. By using advanced search engines, 'scientific' matching services, and proprietary algorithms, dating sites instantly find compatible matches based on values, personality styles, attitudes, interests, race, religion, gender, and ZIP codes (Mitchell, 2009). These

[1] School of Criminal Justice, Center for Law and Justice, 5th Floor, 123 Washington Street, Rutgers University, Newark, New Jersey 07102-3094, USA. Email: aunshul@pegasus.rutgers.edu

digital environments of anonymity and flexibility allow daters to test pluralistic ways of being that are instantaneous, alterable, and open to interpretation, making online dating attractive and stimulating to customers (Hitsch et al., 2005; Wang & Lu, 2007).

Not surprisingly, these qualities have resulted in the proliferation of the online dating sector since the mid-1990s, so much so that there are approximately 1,400 dating sites in North America today, such as Match.com, eHarmony.com, Chemistry.com, and Lavalife.com to name a few (Close & Zinkhan, 2004; Scott, 2009). US daters spent approximately $245 million on online personals and dating services in the first half of 2005 (OPA 2005). The online dating industry generated revenues of $957 million in 2008, making it the fourth highest grossing internet industry after online gambling, digital music, and video games (Epps et al., 2008; McMullan & Rege, 2009; Mitchell, 2009). In fact, the online dating sector is anticipated to generate $1.049 billion in 2009 and is expected to grow at a rate of 10% annually, with projected revenue of $1.9 billion by 2012 (Mitchell, 2009). This successful industry, however, is plagued by cyber crimes, such as romance scams and identity fraud. According to the National Consumers League (NCL), the average victim of a 'sweetheart swindle' lost more than $3,000 in 2007 (NCL 2008; BBC 2007). The Internet Crime Complaint Centre's (IC3) 2007 Internet Crime Report found that online dating fraud was one of the most commonly reported complaints in the ever-rising internet fraud claims (IC3 2007; Mitchell, 2009). Reliable victimization statistics, however, do not exist for several reasons. As King and Thomas (2009) note, romance scams are international in scope and no centralized database tracking victims and their losses is currently available. Furthermore, law enforcement bodies only receive a fraction of all scam complaints, either because victims are embarrassed after being duped, or because they do not realize that they have been swindled (King & Thomas, 2009). While the estimates of victimization are rough at best, online daters are prime targets of romance scams and identity fraud, and thereby warrant special attention.

In the context of this paper, cyber crime is defined as any crime (i) where ICTs may be the agent/perpetrator, the facilitator/instrument, or the victim/target of the crime and (ii) which may either be a single event or an on-going series of events (Rege-Patwardhan, 2009; Symantec 2007). This definition encompasses both the duration of the crime as well as the roles (perpetrator, facilitator, and victim) of ICTs in cyber crimes. Cyber criminals are offenders who (i) are driven by a range of motivations, such as thrill, revenge, and profit, (ii) commit and/or facilitate cyber crimes, (iii) work alone, in simple partnerships, or in more formalized settings, and (iv) have varying levels of technical expertise (Rege-Patwardhan, 2009; Rogers, 2005; Wall, 2007).

This paper explores cyber crimes at dating sites to determine their organizational dynamics. The first section discusses romance scams, which involve fake profiles, fraudulent e-mails, and money orders, gifts, and reshipping of goods. The second section examines identity fraud occurring via dating sites. The third section examines the organizational characteristics and sophistication of various online romance scammers. Fourth, a scammer profile is offered based on skills, resources, scam-cultures, and rationales. The fifth section identifies how technology, cyberspace, and the poorly regulated internet dating industry permit fraudsters to organize and operate romance scams successfully. The paper concludes by stating how this study contributes to the general understanding of cyber crime and of life in cyberspace, and suggests related areas for further research.

Methods

Because data about cyber crimes at dating sites is not readily available from case law or field studies, document analysis is the research method of choice. This method is appropriate for several reasons. First, document analysis fits nicely with the exploratory nature of this research. As Dantzker and Hunter (2006) note, documents assist in discovering "why or how an event occurred and whether such an event could happen again" (p. 74). Indeed, documents allow the examination of cyber criminals, online crimes, and their properties. In addition, this method involves gathering and analyzing preexisting text in different ways so as to answer different research questions than originally intended. Regardless of the context and content of earlier documents, data can be reorganized and analyzed to specifically address the goals of this paper. Second, data on the phenomenon of cyber crime and online dating is not easily available through other methods. Finding romance scammers to interview or survey is nearly impossible because they belong to an underground culture that is unknown or inaccessible. Third, acquiring access to online deviant interaction requires technical expertise and covert observation, which are beyond the scope of this exploratory research and raise ethical issues. Finally, interviewing law enforcement personnel and dating industry representatives is equally challenging. The former are often hesitant to disclose confidential case information, which may include up to date counter strategies, digital evidence and equipment, and the implementation of social control efforts. Most dating industry representatives are reluctant to disclose scam cases for two reasons: (i) fear of being perceived as either vulnerable to scams, which, in turn, encourages further fraud, and (ii) public knowledge of scam activities creates market credibility issues, and drives customers away from established services, thereby benefiting competitors.

Documents published over a nine year time period, 2000 to 2009, were examined. This time frame was selected as the occurrence of cyber crime in the online dating arena was a recent phenomenon. The majority of the data gathered for this research came from online sources. The internet was a global medium and sped the flow of information, providing an abundance of documents from all over the world. The Google search engine was used to collect data because it was the premier search tool and offered three advantages over other search engines such as Yahoo and AltaVista. First, it coded more pages and created a larger index, which was an important factor when detailed research was being conducted. Second, Google presented fresh data by crawling the Web about once a month, adding fresh websites and dropping expired ones. Finally, Google used its "PageRank" technology, which was a numeric value that represented the importance of a website. As such, documents and web pages that were the most relevant to this research were obtained. Twenty keyword combinations such as "internet dating scams", "online dating fraud", "romance 419 scams", and so on (Table 1) were used and the collected data was sorted around four intersecting themes: online dating, scams and frauds, the organization of cyber criminals, and scam prevention and regulation.

Table 1. Twenty keyword combinations used in Google

"internet dating statistics"	"internet dating scams"	"online dating fraud"	"romance 419 scams"
"internet dating" + "organized crime"	"romance scam" + "crime ring"	cyber crime + "internet dating"	"internet dating" + "anti scam"
"online dating" + "social engineering"	"romance scammer database"	"fake profile" + "online dating"	"romance scam" + Nigeria
"romance scam" + Russia	"internet dating" + "identity fraud"	"romance scams" + pictures + photo	"internet dating" + "scammer profile"
scammers + "neutralization techniques"	"romance scams" + "law enforcement"	"romance scams" + regulation	"romance scams" + government

Documents were sampled until "thematic saturation" was achieved. Saturation occurred when the themes identified in the documents began to repeat themselves and subsequent documents did not yield new themes. In this study, thematic saturation occurred with a sample of 100 documents per keyword phrase. In general, Google searches returned 10 'hits' (links to websites or documents) per page, returning a vast number of articles per keyword search (anywhere from 74 to 2,090,000). The first 10 pages, i.e. 100 documents (thematic saturation criterion) were used for each of the 20 keyword combinations to obtain a total of 2000 sample documents. These articles, however, varied in relevance and length, and were also repetitive. The actual sample size was thus much smaller and comprised approximately 170 documents. Overall, this procedure was a consistent means of collecting data and ensured that each category was given equal weight and consideration.

While internet documents were easy to access, use, and link, and were presented in dynamic ways through video clips, sound bites, and animations, there were potential problems with quality control, accuracy of discovery, and consistency of documents over time (McMullan & Rege, 2009). These issues were handled by relying primarily on authenticated websites such as news sites [i.e. LATimes.com], anti-scam sites [i.e. RomanceScams.org], and government sites [i.e. U.S. Department of Justice.], indexing every relevant article's uniform resource locator (URL), creating a registry of all sources, and triangulating multiple sources to cross check information and to look for missing data (Neuman, 2003). This analysis adequately captured the properties of cyber criminal organization, and the operation of online romance scams and identity fraud. Using a different search engine (Yahoo or AltaVista) and a different set of keyword combinations, however, could have resulted in different articles that provided new information and a different analysis. Future research could repeat this study using other search engines and keywords to generalize the findings of this research.

Romance Scams

Romance scams, or 'sweetheart swindles', are an emotionally devastating type of fraud, as scammers make their victims believe they have strong feelings for them; the

romance component of the scam acts as a bait to lure victims, before committing other types of fraud, such as identity theft and financial fraud (Arms, 2010). While other scams, such as lottery scams and employment scams, are somewhat less personal, romance scams lower victims' defenses by appealing to their compassionate side (ScamWatch.gov.au 2010). Romance scams have existed prior to the internet era and have taken many forms (CSS, 2010). For instance, victims would receive romantic letters via post, and after establishing correspondence and trust, the scammer inevitably requests money (Arms 2010). The newspaper dating classifieds were also another avenue for conducting romance scams; these were more targeted as scammers knew their victims sought romance and thus were more likely to be entangled in the scam (Arms, 2010).

Romance scams have now shifted online. Dating websites allow fraudsters to "cast their nets wider and disappear more easily than they could have 20 or 30 years ago" (CSS 2010, p. 1). Scammers can now access a larger pool of victims that are geographically dispersed with great ease and anonymity. Like traditional scams, online romance scams not only result in emotional damage, but also cost victims millions of dollars each year (O'Key 2008). Online romance scams unfold as a *process*, often occurring over several months (O'Key, 2008; USDOS, 2007). Scammers use legitimate dating sites as springboards for meeting their victims (IC3 2007). First, a fake profile is thoroughly designed with an "articulately worded essay, a list of hobbies, … a flirtatious tag line and even a quality picture" (Malko, 2007, p.1). Scammers can use photographs that range from low-quality and heavily pixilated photographs to high quality studio shots; often multiple shots of the same model are used, which strengthens the scammer's credibility who can supply limitless photographs at the victim's request (Ghana-pedia.org, 2009).

The second stage involves contact; the scammer almost always initiates communication with the victim. Scammers then establish a strong bond with their victims through constant communication to generate trust, confidence, and romantic liaisons; this phase can last anywhere from six to eight months until the desired trust-level is achieved (O'Key, 2008; USDOS, 2007). Romance scams are gender neutral, equally targeting male and female online daters. At the third stage, scammers request money from victims by narrating tragic or desperate circumstances, such as theft of personal documents during travel, unexpected hospital expenses resulting from sudden accidents or illnesses, or securing funds for travel to meet the victim (BBC, 2007; Cukier & Levin, 2009; IC3, 2007; OSAC, 2005; USDOS, 2007). Furthermore, these circumstances are often sequential; the scammer always needs more financial assistance as the desperate circumstances intensify. The more successful the scammer is in convincing victims of these circumstances, the more the victim is lured into the scam; this 'cycle of lures' continues until victims lose patience or realize they are being duped and stop sending money (IC3 2007). Given the amount of time and effort undertaken by the scammer to set the groundwork and establish trust, many victims do not realize they are being scammed, making this activity profitable for the scammer (USDOS, 2007).

Consider the cases of Patrick Giblin, Steven Coffman, and Terry McCarthy. Giblin was charged in 2005 for defrauding approximately 130 women using dating sites such as Quest Personals, Lavalife, Intimate Connections, and Private Lines, to feed his gambling habits (Kouri, 2006; USDOJ, 2005; Lovefraud.com, 2009). He swindled a total of $320,241 from victims in New York, Virginia, North Carolina, Georgia, Florida, Ohio, Tennessee, Texas, and Missouri (Kouri, 2006; LoveFraud.com, 2009; USDOJ, 2005). To enhance his credibility, Giblin claimed he was a law enforcement officer and that his father

and brother were also employed with the criminal justice system (LoveFraud.com, 2009). After initiating contact online, he cultivated a telephone rapport with each victim over several days or weeks. He would then declare his interest in pursuing a romantic relationship and falsely promise to end his victims' loneliness (Kouri, 2006; USDOJ, 2005). Eventually Giblin requested financial assistance for relocation to each victim's community; he asked the women to wire him the money via Western Union (Kouri, 2006; USDOJ, 2005).

Steven Coffman was deceived by the Russian scammer 'Elena Inyutina'. They met through an American-based dating website and within a short e-mail exchange, Elena professed her love for Coffman: "I feel you Steve, we are one in heart, spirit, soul mates" (Holguin 2005, p. 1). She requested an in-person meeting and Coffman sent $2,000 for her airfare and visa (Holguin, 2005; Nelson, 2005; Pressbox.co.uk, 2005). When Coffman went to greet his sweetheart at the Sky Harbor Airport in Arizona, Elena never came. When he searched for her on the internet, he found Elena on several Russian Blacklist websites, where she had been titled the "queen of Russian scammers" (Pressbox.co.uk, 2005, p. 3). He discovered that Elena had been scamming several men since 1999 and had used different names and locations (Pressbox.co.uk, 2005). When Coffman contacted the Tempe Police, the Federal Bureau of Investigation (FBI), and the Internet Fraud Complaint Center (IFCC), he was not given any assistance (Nelson, 2005, Pressbox.co.uk 2005). Scammers such as Elena were charming and lured innocent victims into their scams with ease; as Coffman stated: "I never had a woman talk to me like this ever in my life. It wasn't hard for me to fall in love with her. She seemed so perfect" (Nelson 2005, p. 1). These romance scams often originated in Russia's internet cafés where women enticed American men with photos and emails, "suck[ed] out $3,000 to $5,000 [from them, and] then simply disappear[ed]" (Holguin 2005, p. 1). While Giblin and Inyutina acted individually, other scams displayed more organizational sophistication.

Romance scams were also conducted by pairs of individuals. The 2001 fraud against Terry McCarthy was a case in point. McCarthy searched internet sites for a possible Russian love match. Anna Lazarev responded; after a few email exchanges, McCarthy sent her funds so that she could visit him (Smh.com.au, 2004). She kept the money and stopped communication. Unlike most victims, however, McCarthy pursued matters with the Russian government. He wrote a letter directly to the Russian president Vladimir Putin asking that Anna be brought to justice (Smh.com.au, 2004). Putin ordered an investigation, which revealed that Anna and her spouse, Yuri Lazarev, were running the scam (Womenrussia.com 2004). Initially, the Russian couple used Anna's real name and photos to lure men, but as the scam grew in size and scope, they began to use aliases such as "Magdeeva, Marina Chumachenko, Vasilisa Schelkonogova, Anna Porfireva, Olga Trophimova, and many others" (Womenrussia.com 2004, p. 1). The couple also hired female acquaintances to collect wire transfers, as well as women to write romantic and flirtatious messages to victims from all over the world (Womenrussia.com, 2004; Smh.com.au, 2004). The Lazarev duo netted approximately $394,500 over two years by duping about 300 men from Australia, New Zealand, Canada, the United States and other Western countries (Smh.com.au, 2004). Once the payments were made, the 'dream girl' vanished. When Yuri and Anna Lazarev were apprehended, police found detailed biographical information for at least 70 victims (Agencyscams.com, 2006).

Another romance scam operated as a network in Nigeria. These scam networks recruited members based on skill and speed; new members were recruited after being

spotted at cyber cafés (Dixon, 2005). Several members comprised this scam network. First, communicators worked in cyber cafés from "10:30 p.m. until 7 a.m., so [that they could] work in peace" (Dixon, 2005, p. 1). During these extensive shifts, they extracted thousands of American e-mail addresses and sent off 500 fraudulent e-mails daily, some of which were romance scams (Dixon, 2005). Other members were responsible for setting up profiles, using pictures from modeling websites worldwide. Members also included college graduates who composed romantic letters that were disseminated to victims (Dixon, 2005). This collective effort resulted in the scam network receiving about seven replies daily, and as one member noted: "When you get a reply, it's 70% sure that you'll get the money" (Dixon, 2005). Nigerian scammers generated approximately $45 million every year through these love scams (DeBrosse, 2008).

Each type of criminal organization greatly benefits through the use of ICTs. Loners can utilize ICTs to target victims; the combined strength and efforts of hackers is unnecessary (Brenner, 2002). Small-scale scam groups with similar goals can cooperate with greater ease and speed. Hierarchy disappears, paving the way for a lateral networked structure, with loosely-structured sub-networks and global coalitions that are transitory and goal-specific in nature (Brenner, 2002). These criminal organizations often use romance scams as a precursor to other crimes, such as reshipping stolen goods, financial fraud, and identity fraud.

Identity Fraud

In addition to direct emotional and financial damage, romance scams affect victims indirectly. While these victims may not encounter the scammer, their identities are exploited in various sweetheart swindles. Identity is a complex and multi-faceted concept that can be divided into three categories: (i) personal: internalized view of identity that relates to a person's sense of self, (ii) social: externalized view that concerns the way that a person is viewed by others, and (iii) legal: the manner in which the accumulation of information distinguishes one person from all others (Finch, 2007). Thus, personal and social identity are concepts of inclusiveness, whereby individuals establish group membership through similarity to others, while legal identity differentiates individuals from others and is a means of establishing individuality and personhood (Finch, 2007). Furthermore, personal and social identity evolve as individuals change "on the journey through life whereas legal identity is immutable and permanent" (Finch, 2007, p. 31). Identity fraud involves the impersonation of another person for a particular purpose after which imposters reverts to their own identity, while identity theft involves the total abandonment of one identity and the complete assumption of another, distinct identity (Berg, 2009; Finch, 2007). While identity theft and fraud occur in the physical world, cyberspace permits imposters to shield their true identities and take on numerous aliases with greater ease; just as "consistency of identity is expected in the real world, opacity of identity is the norm in the virtual world" (Finch, 2007, p. 37). Identity fraud involves the appropriation of legal identity, which is concerned with the ability to authenticate claims to be a particular individual.

Romance scammers required pictures to set up their profiles, which they acquired from a variety of sources (Finn & Banach, 2000). Nigerian-based romance scams typically utilized photographs from modeling sites, such as Focus Hawaii (Datingnmore.com, 2004). Scammers patiently sifted through various photo galleries and selected the most lucrative pictures for their profiles. Alternatively, scammers took photos and profiles of

innocent customers registered at legitimate dating sites to create a deliberately misleading impression as to aspects of their identity (Datingnmore.com, 2004; Finch, 2007). The absence of in-person interaction and other sensory cues (visual appearance, sound, and so on) available in the real world to authenticate identity contribute significantly to the potential for protecting, modifying, or otherwise misrepresenting identity.

Yet another source for scammers was using easily available images on the internet. Consider the case of Robert Frost, a professional racecar driver in the Grand American Rolex Sports Car Series. In 2007, Frost was tracked down, sent flowers, and recognized at several public airports by women he had never met (DeBrosse, 2008). Unbeknownst to Frost, his photos had been uploaded on several dating sites by romance scammers to lure women; since 2007, Frost's images had appeared on approximately 90 websites, under 80 different e-mail addresses and aliases (DeBrosse, 2008). Mary Leal, an internet security consultant investigating Frost's case, physically travelled to Nigeria and met one 'Robert Frost', a 24-year-old man by the name of George McCall (DeBrosse, 2008). When asked about using Frost's picture illegally, McCall disagreed that he had stolen the photo: "anything (accessible) on the Internet [was] legal" (DeBrosse, 2008, p. 2). Similarly, the abovementioned Lazarev duo had taken pictures of women who had no knowledge that their images were being circulated online as marriage partners, or that victims were being asked for money in their names (Agencyscams.com, 2006). Another form of identity fraud occurred when scammers sent copies of altered passports and US visas to assure victims who doubted their existence and their intent to visit (OSAC, 2005).

The internet also gave romance scammers access to personal information; they were able to sift through official sources in online identity databases to find suitable victims, acquire sufficient information about them, and then assume their identity. Fraudsters who were intent on committing financial fraud targeted individuals that had solid credit ratings and easily accessible credit card or bank account information. In order to pay membership fees at dating websites, scammers engaged in financial identity fraud; they hacked into eBay and similar sites to access credit card numbers (DeBrosse, 2008). Furthermore, they used these stolen credit cards to buy flowers or candy to further demonstrate their love for the victim (Sullivan, 2005). Scammers sometimes required assistance with re-shipping items that were often purchased with stolen credit cards to various Nigerian locations (Sullivan, 2005). As many US merchants were wary of shipping to Nigeria, scammers used their victims as middle-men; one victim had merchandise worth $50,000 sent to her to be reshipped to her partner in Nigeria (Sullivan, 2005). Thus, as Finch (2007) noted, cyberspace weakened the adherence of legal identity to its rightful owner and permitted scammers to access a far wider range of potential victims. Not only did cyberspace offer imposters anonymity and security from detection, it also disassociated them from any accountability, thereby permitting them to act criminally with little remorse and consequence.

Organizing Romance Scams

Law enforcement authorities and the dating industry claimed that romance scams operated as organized crime (BBC, 2007; Enoch, 2008). As one security expert stated: "many of these scammers work together to create enormous fraud rings and share data on how best to scam people" (Enoch, 2008, p. 3). While 'organized crime' has been portrayed as large-scale, enduring 'Mafia-type syndicates with strict hierarchies of authority, an international scope, and involvement in several illicit enterprises, their

prominence has faded as they now comprise only a minority of organized criminal groups (Bullock et al., 2010). Small organized and transient networks of criminals are far more common; they coalesce to commit specific crimes and disband upon their completion (Bullock et al., 2010; McMullan & Rege, 2009). The national police forces in the U.K. and Germany, as well as the European Union have recently adopted this broader definition of organized crime. Are cyber-sweetheart scams conducted as organized crime, crimes that are organized, or crimes that range in organizational complexity? What characteristics of organized crime are evident in these scams? Do ICTs alter some of these characteristics? Addressing these questions requires identifying which organized crime characteristics fit each type of scammer listed above (Table 2).

First, not all the scamming operations were conducted by groups of criminals; several romantic swindles were committed by either individuals working alone or small groups of criminals. For instance, Giblin and Elena duped several victims on their own, while the Lazarev scam initially enjoyed success with just two members. Online scam networks, such as the Nigerian scam ring, extended over space and time using ICTs, required "less personal contacts and thus less relationships based on trust and enforcement of discipline between criminals" (Council of Europe, 2004, p. 9). In fact, ICTs favored those organizations that were already based on flat-structured networking, with "loose collaborative criminal [sub-] networks" (Council of Europe, 2004, p. 9; McAfee, 2005). Each sub-network worked together to successfully implement cyber crimes. What organizational structure did scam networks exhibit?

Online romance scam networks did not have strict membership criteria; the Lazarev group and the Nigerian network were flexible and hired members as needed. Regardless of the size of membership, group codes were non-existent; the only common goal shared by all scammers was to make money. Furthermore, scammers did not exhibit the property of continuity; scammers generally vanished when they reached their monetary goals or when they were exposed. Also, scammers engaged in extensive planning to ensure the smooth execution of their crimes; they groomed their victims for extended time periods and sweet talked them into giving up their finances. But what organizational structure did these scam networks exhibit?

Lemieux (2003) identifies the main roles inherent in most criminal networks of any size. At the core of a criminal network are the *organizers*, who determine the nature and scope of activities (Lemieux, 2003). The *extenders* are responsible for the expansion of the criminal network. They recruit new members and encourage collaboration with other illegal businesses, government and justice. In scam networks, it appeared that the same individuals acted as both organizers and extenders, recruiting members with varying skills (typing, English proficiency, hacking) as needed to ensure the successful overall operation of the criminal enterprise.

The *executors* are responsible for carrying out the objectives of the organizers. They implement the attacks according to the plans laid out by the organizers and possess the specialized skills necessary to successfully carry out the operation. In romance scam networks, executors were those who could speak foreign languages, compose flirtatious letters, write e-mails, and speak on the phone with their victims to keep them engaged in the scams (CBC, 2008). *Enforcers* are the protectors of the criminal network and they take the necessary measures to ensure compliance from victims (Lemieux, 2003). While the use of corruption was not evident in the above scam examples, the use of emotional blackmail and extortion were evident. For instance, when victims were unwilling to send money,

scammers often said, "you don't have any feelings for me", "I thought we had a real relationship here", or "you're heartless" to lure the victim back into the scam (Netcred.co.uk, 2006). In cases where scammers were exposed, they swore that they fell in love with the victim. This technique was effective because victims already had a strong bond with their scammers (Romancescams.org, 2008a). In scams where webcams were used by victims, fraudsters recorded webcam videos and later used these to extort money to prevent releasing films and pictures to porn sites (Romancescams.org, 2008b).

Money movers collect money from the victims and return it back to their criminal enterprise. The money mules in scam networks picked up monies wired through Western Union. Finally, there are *crossovers* who are part of the criminal network but also belong to legitimate governmental, financial, or commercial sectors. Scam victims are often convinced of the authenticity of numerous government documentation bearing official government letterhead, stamps, and seals (Cukier & Levin, 2009). As such, crossovers provide invaluable insider access and legitimacy, thereby contributing to the effectiveness of the criminal organization and the romance scam. While no explicit information about crossovers was found in the above-mentioned cases, these individuals may be recruited as necessary by the network to provide false official documentation, such as passports and visas, to enhance the scammer's credibility.

Table 2. Typology of Romance Scammers and Identity Fraudsters

Criminal Organization	Bonds & Structure	Division of Labor	Non-technical Skills	Technical Skills	Neutralization Technique	Evasion Technique
Individual	- N/A	- N/A	- Patient - Social skills (smooth-talking, trust-building) - Routine	- Basic computer skills - Fake profile/ image	- Denial of victim	- Anonymity
Small Group	-Strong and weak bonds -Long-lasting and transient alliances -Decentralized	- Organizers/ extenders - Executors - Money movers	- Patient - Social skills (smooth-talking, trust-building) - Routine	- Basic computer skills - Fake profile/ image - Victim databases	- Denial of victim - Denial of injury	- Anonymity - Flexibility & dynamic (re)organizatio n
Large-scale Network	-Weak bonds -Transient -Decentralized	- Organizers - Extenders - Executors - Enforcers - Money movers - Crossovers	- Patient - Social skills (smooth-talking, trust-building) - Routine - Scam culture (resource sharing, training)	- Basic computer skills - Fake profile/ image - Victim databases - Mass e-mail dissemination	- Denial of victim - Denial of injury - Appeal to higher loyalties	- Anonymity - Flexibility & dynamic (re)organizatio n - Autonomous operation - Exposure of sub-networks instead of entire network

There are several advantages arising from this networked structure in regard to criminal events. First, there is no head authority in control; sub-networks have the freedom to operate autonomously. Second, the loose connections within the network allow for flexibility, which facilitates the "rapid reorganization of criminal activities in

response to changing consumer demand and law enforcement activities" (Schloenhardt, 1999, p. 13). Not surprisingly, these networks are sometimes described as "disorganized", and it is precisely this quality that makes them dynamic and efficient: "if a node or hub disappears, nodes may simply move their connections to others", thereby exhibiting regenerative tendencies (Yoo, 2005, p. 2). Finally, the network model is less vulnerable to social control. Only smaller units are exposed to policing agents, leaving the rest of the network intact: "free-scale networks remain remarkably immune to attack; randomly destroying nodes will not cause [the entire network] to collapse" (Yoo, 2005, p. 2). Having examined the organizational dynamics of scammers, the next section discusses properties that are specific to online romance scam operations.

Online Romance Scammer Profile

Regardless of their organizational sophistication, scammers exhibited certain common traits. First, they were patient in grooming their victims. They spent time selecting and stealing photos that would make their operations successful, establishing victims' trust, and sweet-talking them into the scam. This six to eight month process clearly demonstrated that scammers were enduring, rational, planned, and coordinated in their crimes.

Second, unlike cyber crimes such as hacking into servers, installing malware, and manipulating software programs, which required technical expertise, online scamming required basic computer skills and an internet connection. Scammers did not have to hack into dating sites to create accounts; they easily created dating profiles at numerous matchmaking sites that had little to no security or background verification checks. More important skills included social skills; they were trained in the art of smooth-talking victims, establishing trust, and building confidence. Some scam networks may have hired technologically savvy individuals to hack and acquire credit card information resulting in identity fraud. These temporary recruits resulted in transient and dynamic network structures.

Third, scammers followed routines thoroughly. Scammers worked six-hour shifts and engaged in an extensive division of labor, with each unit responsible for a specific task. Members were responsible for mapping out online courtships, planning different scenarios that may occur during real-time conversations, and when to introduce tragic circumstances (CBC, 2008). Some networks hired trained psychologists who assisted in further psychologically trapping victims (CBC, 2008). Scammers had a goal of retrieving two or three Western Union wires from victims each week, with a monthly expected take of about $1,000 (DeBrosse, 2008). This thorough routine and dedication permitted scammers to successfully defraud millions of victims. Scammers made $30,000 in 'good months', which were spent on "clothes, hotel rooms, and Dom Perignon at 'VIP' clubs" (Brulliard, 2009, p. 2).

Fourth, online romance scam networks subscribed to a 'scam-culture'. Many individuals belonged to groups of scammers who pooled their money, shared internet access and resources, and trained newcomers to the art, some as young as 6 years old (DeBrosse, 2008). Romance swindlers acquired all the necessary tools to commit their scams: "formats, or 'FMs' for letters; 'mailers', or accounts that send e-mails in bulk; and huge lists of e-mail addresses, bought online" (Brulliard, 2009, p. 2). Scammers rented computers for "60 Nairas each (about 50 cents) for 30 minutes of browsing, [and] correspond[ed] with dozens of different women at once in Western countries" (DeBrosse, 2008, p. 1). The city of Lagos in Nigeria served as a hub for romance scams; here,

scammers in internet cafés were trained in social skills. With the increasing availability of wireless internet services, however, fraudsters could also commit their crimes from private residences (Bruillard, 2009).

Finally, online scammers engaged in three main neutralization techniques to rationalize their activities before bilking their victims. The members of the Nigerian-scam network rationalized their acts by employing the 'denial of victim' technique, where the scam was viewed as a punishment towards a deserving person; their prey was "avaricious and complicit" (Dixon, 2005, p. 1). In fact, scammers had their own anthem titled 'I Go Chop Your Dollars', which states: "You be the mugu [victim], I be the master… I go chop your dollar, I go take your money and disappear. 419 is just a game, you are the loser I am the winner", which clearly demonstrated that scammers subscribed to the 'sucker mentality' (Dixon, 2005, p. 1; Finckenauer, 2007). Another Nigerian scammer anthem states: "my maga don pay/Shout alleluia", which celebrates that a victim (maga) sent money (Brulliard, 2009). Other scammers, like McCall, did not believe that they were engaging in any illicit conduct when using other individuals' identities. They subscribed to the 'denial of injury' neutralization technique as they were not bilking these individuals and therefore not causing any real harm to them. Finally, scammers used the 'appeal to higher loyalties' neutralization technique, where scamming in criminal networks was embedded in a larger scam culture. Here, scammers exhibited loyalty to the norms and goals of their own criminal network; they subscribed to criminal mores such as weekly goals of acquiring money, supporting each other, sharing and pooling resources, and training novices.

Discussion

Several factors compound the problem of online romance scams. First, the online dating industry is hardly subjected to any regulation and background verification checks are seldom conducted (BBC, 2007; McRae & McKnight, 2007). Most dating sites handle scammers through a 'report abuse' feature on their websites. The onus of protection is on online daters and not on police or dating sites (Tracy, 2008). Few sites do offer proactive strategies such as screening for patterns of scammer behavior and deleting those profiles immediately (Tracy, 2008). Australia's Cupid Media is a case in point. This dating website gets approximately 15,000 new profiles everyday, of which 3,000 are rejected based on their poor use of English and unrealistic profile photos (Bentley, 2009). PerfectMatch.com looks for scammers who blast email messages to thousands of people right after creating their accounts (Mitchell, 2009). PerfectMatch.com also looks for certain keywords and phrases that is indicative of scammers. eHarmony has partnered with *Iovation*, which offers "Reputation Manager, a service that gathers information on individuals' illicit activity from online dating and other sites and makes it available to subscribers" (Mitchell, 2009, p. 5). True.com blocks IP addresses associated with specific countries, such as Nigeria, which filters approximately 20% of applicants (Mitchell, 2009). This site also runs criminal background checks on everyone who subscribes to its service, blocking roughly 80,000 felons from subscribing in 2008 (Mitchell, 2009). Industry experts, however, agree that most background checks would be costly with little increase in safety: "a very basic background check costs about $10, … [but] most scammers would still be able to get around that layer of security" (Enoch, 2008, p. 4). For instance, scammers use stolen credit cards, rendering background checks on stolen identities useless (Mitchell, 2009).

Furthermore, several law enforcement databases do not communicate with each other, questioning the legitimacy of background checks (Mitchell, 2009).

Second, when victims do come forward, they are rarely offered any assistance from law enforcement agencies. Issues of vagueness in jurisdiction, lack of international collaboration, and low priority of dating scams work against victims of sweetheart swindles. While the FBI, US embassies, and local police issue warnings about dating scams, little assistance is offered beyond these admonitions. In some instances, when victims file a complaint with the authorities in countries where the scam originated, they receive a call back from someone claiming to be a police official. This official will then state that their monies have been recovered, but a fee payment is necessary to get the funds back, resulting in yet another scam (Cukier & Levin, 2009). This scenario is problematic not only because the victim is defrauded again, but also because the victim mistrusts officials thereby contributing to the scam underreporting rate. Furthermore, this situation also suggests the strong connections between crossovers in the law enforcement sector and members of the scam network. Some international collaboration, however, do exist. The Nigerian government works with Queensland Police using an online reporting system; Australian victims can report scams directly to Nigeria's Economic and Financial Crimes Commission (EFCC) (Moses, 2009). This partnership has lead to the arrest and prosecution of 10 Nigerian fraudsters, whose assets will be used to repay victims (Moses, 2009). Other anti-scam websites, such as romancescams.org and ghana-pedia.org offer support services, scam education, and incident reporting. These sites also offer scammer data bases that list the fraudster's profile nickname and 'real' name, e-mail address, phone number, location, and address. Potential victims can cross-check their sweetheart's information against these databases, identify any possible scams, and report the fraud, thereby protecting themselves and others from being victimized. Ghana-pedia plans to initiate a new dating page that will filter out the genuine profilers from the bogus ones, using several confirmation tactics, such as meeting with a Ghana-pedia representative personally and supplying authenticated identification details (Ghana-pedia.org, 2009).

Conclusion

Literature on cyber crime has examined cyber terrorism (Blane, 2002; Lewis, 2004; Taylor et al., 2006), cyber extortion (Bednarski, 2004; McMullan & Rege, 2009; Paulson & Weber, 2006), online identity theft (Jewkes, 2003; Berg, 2009; Finch, 2007), online child pornography (Jenkins, 2001; Wells et al., 2007; Wortley & Smallbone, 2006), organized cyber crime (Brenner, 2002; LeBeuf, 2001; McAfee, 2007), and legal and policing challenges (Nhan & Huey, 2008; Pattavina, 2005; Smith et al., 2004), to name a few. Online dating crimes offer yet another context to further comprehend the many faces of cyber crime, and their properties and consequences.

First, this paper examines how cyber criminals organize and operate to commit online romance scams. Conventional theories for criminal organization were created before the advent of cyberspace and technology, and have therefore not considered their impact on the organization of criminals. This research offers a preliminary examination of online criminal structure using a socio-organizational level of analysis. It examines how digital environments influence cyber criminal organization. ICTs change the face of crime allowing cyber criminals to use technology to commit deviant acts, by offering anonymity, increased flexibility and transience, better efficiency, and speed, which cyber criminals use to organize themselves and their acts. The characteristics of cyberspace that facilitate crime

can be accounted for by the acronym SCAREM (Stealth, Challenge, Anonymity, Reconnaissance, Escape, and Multiplicity) (Newman & Clarke, 2003). Indeed, cyber criminals are invisible and anonymous in cyberspace, difficult to detect, highly motivated and rationally choose their targets, and can easily replicate their crimes. Scammers can attack from a distance, which makes tracking them difficult. Scammers can be *anyone* in cyberspace; they can easily change names, emails, photos, and list themselves on different dating sites as being of different gender, race, age, and sexual orientation. These fraudsters are purposeful in their choice of victims, targeting those who are emotionally vulnerable in order to extract funds. Finally, once scammers have their initial profile and tragic circumstances established, they can simultaneously and repeatedly victimize online daters.

Second, this paper also illustrates the impact of cyber crime on victims. Not only do victims of romance scams suffer emotional harm, but, as Berg (2009) notes, their sense of self, trust, and autonomy is also violated. Victims experience a range of negative emotions, such as anger, resentment, fear, anxiety, and depression (Berg, 2009). Furthermore, victims of romance scams feel embarrassed and believe that they are responsible for their victimization, which impacts their sense of trust in themselves, potential online matches, and the overall online networking experience. In addition to online daters, dating websites also experience victimization; public knowledge of victimization creates market credibility issues, and drives daters away from their business towards other dating sites. By identifying the assortment of cyber crimes at dating sites and creating a typology of these crimes, this paper addresses the prevalence of cyber criminality, and the benefits offered to cyber criminals, at and by online dating environments. By understanding how cyber criminals exploit dating site vulnerabilities and circumvent protective measures, this research contributes to the areas of internal and external security issues in the online dating sector.

Finally, this exploratory research can be used as a foundation for more specific studies into the area of cyber crime at dating sites. One area is the creation of phony dating sites by cyber criminals. Here, legitimate daters pay service fees to create an account on the fake dating site, as well as for each email or message they send and receive. Scammers create false profiles on the bogus site and send love-laden messages to their victims in an effort to extract victims' monies (ScamWatch.gov.au, 2010). Second, researchers can explore variations in romance scams. For instance, a recent twist in the romance scam involves the United States army. In this case, scammers pretend to be US soldiers serving in Iraq or Afghanistan, take on their true ranks and names, and link it to freely available images of soldiers on the internet (Army.mil, 2010). These scammers exploit the emotions and patriotism of their victims, asking them to send funds for laptops, international telephones, and transportation fees (Army.mil, 2010). A third area of research involves studying other types of fraud associated with online romance scams. Romance scammers often engage in other scams, such as "Nigerian Emergency Scams, Plane Ticket and Visa Scam, Nigerian 419 Scams, Fake Police Scams, Cashing Money Order Scams, Lottery Scams, Phony Inheritance Scams, and Job Scams", which indicates that their organizational sophistication and range of criminal activity needs further study (ODST, 2009, p. 1). Finally, researchers could study other crimes linked with romance scams. In 2010, a British national travelled to West Africa to meet his online 'sweetheart'. This romance fraud, however, was not operated by a scammer, but was generated by an organized crime group (SOCA, 2010). Upon arrival, the victim was kidnapped, assaulted, and held prisoner until a release-ransom was paid. Since 2007, there have been reports of Australian, Belgian, and German nationals being kidnapped as a result of online romance

scams (SOCA, 2010). The connection of organized crime groups to online romance scams is an area that is understudied.

To conclude, online romance scams are here to stay. The booming online dating industry with its ever increasing membership continues to offer scammers with a ready pool of suckers that are ideal for exploitation. As Nigerian scammers state: "every day, another maga is born in America" (Brulliard, 2009, p. 3). The few and weak countermeasures, the ease of creating dating profiles, an increasing supply of victims, the reluctance of reporting victimization, their social skill prowess, their rationales and justifications, and their untouchable and anonymous status, grants these romance scammers a sanctuary in cyberspace.

Acknowledgement:

The author thanks Dr. Ronald Clarke for his insightful comments that run throughout this paper. Any shortcomings, however, are the author's.

References

Agencyscams.com (2006). *Arrests*. Retrieved January 22, 2009, from http://www.agencyscams.com/Arrests.html

Arms, S. (2010). *Romance Scam: Scammers Feign Affection to Commit Fraud*. Retrieved April 10, 2010, from http://crime.suite101.com/article.cfm/romance_scam

Army.mil (2010). *CID warns of Internet romance scams*. Retrieved April 10, 2010, from http://www.army.mil/-news/2010/03/23/36242-cid-warns-of-internet-romance-scams/

BBC (British Broadcasting Corporation) (2007). *UK police in Nigerian scam haul*. Retrieved September 7, 2008, from http://news.bbc.co.uk/1/hi/uk/7027088.stm

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

Bentley, A. (2009). *Caught in Love's Cruel Web*. Retrieved October 20, 2009, from http://www.brisbanetimes.com.au/technology/security/caught-in-loves-cruel-web-20091016-h0lk.html

Berg, S. (2009). Identity Theft Causes, Correlates, and Factors: A Content Analysis. In F. Schmalleger & M. Pittaro. (Eds.), *Crimes of the Internet* (pp. 225-250). New Jersey: Pearson Prentice Hall.

Blane, J.V. (2002). *Cyberwarfare: Terror at a Click*. NY: Novinka Books.

Brenner, S. W. (2002). Organized Cyber crime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law & Technology, 4*(1), 1-41.

Brulliard, K. (2009). *Worldwide Slump Makes Nigeria's Online Scammers Work That Much Harder*. Retrieved September 1, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2009/08/06/AR2009080603764.html

Bullock, K., Clarke, R.V. & Tilley, N. J. (2010). *Situational Prevention of Organized Crimes*. Willan Publishing, UK.

CBC (Canadian Broadcasting Corporation) (2008). *Cyber love lost in Russian bride scam*. Retrieved March 2, 2009. Online at http://www.cbc.ca/canada/montreal/story/2008/02/13/qc-russian-dating-0213.html

Close, A. & Zinkhan G. (2004). Romance and the Internet. The E-Mergence of E-Dating. *Advances in Consumer Research, 31*. 153-157.

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

Cukier, W. & Levin, A. (2009). Internet Fraud and Cyber Crime. In F. Schmalleger & M. Pittaro. (Eds.), *Crimes of the Internet* (pp. 251-279). New Jersey: Pearson Prentice Hall.

CSS (CyberStreetSmart.org). (2010). *Other Types of Online Romance Scams*. Retrieved April 10, 2010, from http://www.cyberstreetsmart.org/dating/dating_other.html

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

Datingnmore.com (2004). *Nigerian Dating Scam, aka Romance Scam*. Retrieved September 7, 2008, from htpp://www.datingnmore.com/fraud/scam_database.htm

DeBrosse, J. (2008). *ID theft victim becomes pawn in dating scam*. Retrieved April 4, 2009 from http://www.daytondailynews.com/n/content/oh/story/news/local/2008/04/06/ddn040608scammers.html

Dixon, R. (2005). *Nigerian Cyber Scammers*. Retrieved April 5, 2009, from http://www.latimes.com/technology/la-fg-scammers20oct20,0,301315.story?page=1&coll=la-tot-promo

Enoch, J. (2008). *Love's Labors Looted: Internet Dating Scams Can Get Expensive*. Retrieved September 7, 2008, from http://www.consumeraffairs.com/news04/2008/07/eharmony.html

Epps, S. et. al (2008). *US B2C Online Paid Content: Five-Year Forecast*. Forrester Research Inc.

Finckenauer, J. (2007). *Mafia and Organized Crime*. Oxford: Oneworld Book.

Finch, E. (2007). The Problem of Stolen Identity and the Internet. In Y. Jewkes. (Ed.), *Crime Online* (pp. 29-43). Oregon: Willan Publishing.

Finn J. & Banach, M. (2000). Victimization Online: The Down Side of Seeking Human Services for Women on the Internet. *Cyberpsychology & Behavior, 3*(2), 243-54.

Fiore, A. & Donath, J. (2004). *Online Personals: An Overview*. ACM Computer-Human Interaction 2004, Vienna, Austria.

Ghana-pedia.org (2009). *419 – Internet Dating Scams*. Retrieved September 2, 2009, from http://www.ghana-pedia.org/org/index.php?option=com_content&task=view&id=29&Itemid=47

Holguin, J. (2005). *Beware Russian Web-Order Brides*. Retrieved April 4, 2009, from http://www.cbsnews.com/stories/2005/04/14/eveningnews/main688311.shtml

Hitsch, G., Hortacsu, A. & Ariely, D. (2005). *What Makes you Click: An Empirical Analysis of Online Dating*. MIT Solan Research Paper No. 4603-06.

IC3 (Internet Crime Complaint Center) (2007). *2007 Internet Crime Report*. Retrieved April 1, 2009, from http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf

Jenkins, P. (2001). *Beyond Tolerance: Child Pornography on the Internet*. New York: New York University Press.

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

King, A. & Thomas, J. (2009). You Can't Cheat an Honest Man: Making ($$$ and) Sense of the Nigerian E-mail Scams. In F. Schmalleger & M. Pittaro. (Eds.), *Crimes of the Internet* (pp. 206-224). New Jersey: Pearson Prentice Hall.

Kouri, J. (2006). *"Don Juan" Gambler Pleads Guilty to Bilking Vulnerable Women Out of Money*. Retrieved September 7, 2008, from http://www.theconservativevoice.com/article/14664.html

LeBeuf, M. (2001). *Organized Crime and Cyber crime: Criminal Investigations on the Cutting Edge*. Retrieved December 1, 2005 from http://www.cpc.gc.ca/research/ocrime_e.pdf

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

Lewis, J. (2004). Cyber Terror: Missing in Action. In D. Clarke (ed), *Technology and Terrorism* (pp. 145-153). NJ: Transaction Publishers.

Lovefraud.com (2009). Patrick Giblin: Trolling Phone Dating Lines, Taking Money From 132 Women. Retrieved April 2, 2009, from http://www.lovefraud.com/03_trueLovefraudStories/Patrick_Giblin_swindles_100_women.html

Malko, J. (2007). *Fake Profiles*. Retrieved October 2, 2008, from http://www.cupidsreviews.com/article/Fake-Profiles.htm

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

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

McMullan, J. & Rege, A. (2009). Cyberextortion at Online Gambling Sites: Criminal Organization and Legal Challenges. In I. Carr, (Ed.), *Computer Crime – International Library of Criminology, Criminal Justice and Penology – Second Series*. UK: Ashgate Publishing.

McRae, B. & McKnight, J. (2007). Privacy and Online Dating. In *Convenient of Invasive – The Information Age*. CO: Ethica Publishing.

Mitchell, R. (2009). *A well-oiled Internet dating machine can generate well in excess of £140 million a year and has replaced the historic personal ad. What is the secret behind one of the Internet's biggest success stories?* Retrieved May 16, 2009, from http://www.computerworlduk.com/management/online/isp/in-depth/index.cfm?articleid=2069

Moses, A. (2009). *Hardline Nigerian official pledges to arrest the 419 scammers*. Retrieved September 1, 2009, from http://www.smh.com.au/technology/security/hardline-nigerian-official-pledges-to-arrest-the-419-scammers-20090901-f65d.html

Nhan, J. & Huey, L. (2008). Policing through nodes, clusters and bandwidth. In S. Leman-Langlois. (Ed.). *Technocrime: Technology, crime and social control* (pp. 1-13). Oregon: Willan Publishing.

NCL (National Consumers League) (2008). *Love Stinks. Consumer Group Helps Lonely Evade Scams*. Retrieved February 13, 2009, from http://www.nclnet.org/news/2008/sweetheart_swindles_02082008.htm

Nelson, K. (2005). *Tempe man warns of Internet scam that led to heartbreak*. Retrieved September 7, 2008, from http://www.crime-research.org/news/15.04.2005/1161

Netcred.co.uk (2006). *The Sweetheart Scam*. Retrieved September 7, 2009. Online at http://netcred.co.uk/security/sweetheart-dating-fraud.html

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

Newman, G. & Clarke, R. (2003). *Superhighway Robbery: Preventing E-commerce Crime*. OR: Willan Publishing.

ODST (Online Dating Safety Tips.com) (2009). *Top 10 Scams*. Retrieved October 20, 2009, from http://www.onlinedatingsafetytips.com/Top10Scams.cfm

O'Key, S. (2008). *Looking for love? Keep an eye on your wallet*. Retrieved October 2, 2008. , from http://www.cnn.com/2008/LIVING/04/21/romance.fraud/index.html

OPA (Online Publishers Association) (2005). *U.S. Consumer Spending for Online Content Totals $987 Million in First Half of 2005*. Retrieved March 21, 2009, from http://www.online-publishers.org/newsletter.php?newsType=pr&newsId=34

OSAC (Overseas Security Advisory Council) (2005). *Internet Dating Fraud Scam*. Retrieved September 7, 2008, from https://www.osac.gov/Reports/report.cfm?contentID=39785&print

Pattavina, A. (2005). *Information Technology and the Criminal Justice System*. California: Sage Publications.

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

Pressbox.co.uk (2005). *CBS Evening News interview with Steven E Coffman of Family-eStore.com to be aired Russian dating*. Retrieved April 4, 2009, from http://www.pressbox.co.uk/detailed/26727.html

Rege-Patwardhan, A. (2009). Cyber crimes against critical infrastructures: a study of online criminal organization and techniques. *Criminal Justice Studies, 22* (3), 261-271.

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

Romancescams.org (2008a). *About Romance Scammers*. Retrieved April 5, 2009, from http://www.romancescams.org/RS%20About%20Romance%20Scammers.html

Romangescams.org (2008b). *Blackmail with webcam pictures*. Retrieved April 5, 2009, from http://www.romancescams.org/RS%20Blackmail.html

ScamWatch.gov.au. (2010). *Dating and Romance Scams*. Retrieved April 10, 2010, from http://www.scamwatch.gov.au/content/index.phtml/tag/DatingRomanceScams

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

Scott, M. (2009). Multistakers say one online dating site won't do. Retrieved March 10, 2009, from http://www.heraldnews.com/lifestyle/x545172880/Multitaskers-say-one-online-dating-site-wont-do

Smh.com.au (2004). *Bride scam exposed – again*. Retrieved April 4, 2009, from http://www.smh.com.au/articles/2004/11/11/1100021908013.html?from=storylhs

Smith, R., Grabosky, P. & Urbas, G. (2004). *Cyber criminals on Trial*. New York: Cambridge University Press.

SOCA (Serious Organized Crime Agency) (2010). *SOCA Warns of 'Romance Fraud' Kidnap Threat*. Retrieved April 12, 2010, from http://www.soca.gov.uk/news/press-releases/doc_download/96-soca-warns-of-romance-fraud-kidnap-threat.pdf

Sullivan, B. (2005). *Singles seduced into scams online*. Retrieved September 7, 2009, from http://www.msnbc.msn.com/id/8704213/print/1/displaymode/1098

Symantec (2007). *What is Cyber crime?* Retrieved July 3, 2007, from http://www.symantec.com/avcenter/cybercrime/index_page2.html

Taylor, R. W., Caeti, T. J., Loper, D. K., Fritsch, E. J., & Liederbach, J. (2006). *Digital Crime and Digital Terrorism*. NJ: Pearson Education, Inc.

Tracy, J. (2008) *Inside The Online Dating Industry*. Retrieved September 7, 2008, from http://www.onlinedatingmagazine.com/columns/industry/2008/onlinedatingscams.html

USDOJ (United States Department of Justice) (2005). *United States of America v. Patrick M. Giblin*. Retrieved April 4, 2009, http://www.usdoj.gov/usao/nj/press/files/pdffiles/SuperIndict.pdf

USDOS (United States Department of State) (2007). International Financial Scams – Internet Dating, Inheritance, Work Permits, Overpayment, and Money-Laundering. Retrieved February 10, 2009, from http://travel.state.gov/pdf/international_financial_scams_brochure.pdf

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

Wang, H. & Lu, X. (2007). Cyberdating: Misinformation and (Dis)trust in Online Interaction. *Informing Science Journal, 10*.

Wells, M., Finkelhor, D., Wolak, J. & Mitchell, K.J. (2007). Defining Child Pornography: Law Enforcement Dilemmas in Investigations of Internet Child Pornography Possession. *Police Practice and Research, 8*(3), 269-282.

Womenrussia.com (2004) *Internet scammers arrested in Russia*. Retrieved September 7, 2008, from http://www.womenrussia.com/scammers_caught.htm

Wortley, R. & Smallbone, S. (2006). *Child Pornography on the Internet*. Problem-Oriented Guides for Police. Problem-Specific Guides Series. Guide No. 41.

Yoo, J. (2005). *Fighting the New Terrorism*. Retrieved January 14, 2005, from http://www.aei.org/publications/pubID.22735,filter.all/pub_detail.asp