Cyber stalking: An Analysis of Online Harassment and Intimidation

Michael L. Pittaro[1]
Council on Alcohol and Drug Abuse, Allentown, Pennsylvania, USA

Abstract

Our society has come to rely on the sheer size, technological power, and lightening fast speed of the Internet to seek out immeasurable pages of information, explore the unknown, and communicate with virtually anyone, anywhere, and at anytime across the globe. Conversely, the Internet has opened windows of previously unknown criminal opportunities that not only challenge, but also transcend all physical boundaries, borders, and limitations to detect, punish, and diminish what appears to be a mounting problem of global proportion. As such, the Internet has literally become a fertile breeding ground for an entirely new and unique type of criminal offender hereafter known as the cyber stalker – an offender who uses the Internet as a tool or weapon of sorts to prey upon, harass, threaten, and generate immense fear and trepidation in its victims through sophisticated stalking tactics. This paper presents a glimpse into the deviant behaviors and tactics associated with cyber stalking crimes, legislative intervention measures, and preventative initiatives created specifically to curtail this emerging global crime.

Keywords: Cyber Stalking; Harassment; Intimidation; Internet; Deviant behavior.

Introduction

The Internet has undergone rapid growth in this millennium in that it has promoted advances in just about every aspect of society and is available and accessible in practically every corner of the globe (McFarlane & Bocij 2003; Jaishankar & Sankary 2005). The predicted benefits to society are incalculable. The Internet is primarily responsible for developing and enriching global commerce to previously inconceivable heights, fostering remarkable advancements in education and healthcare, and facilitating worldwide communication that was once perceived to be limited and costly (McFarlane & Bocij, 2003; Jaishankar & Sankary 2005). However, the Internet, with its infinite size and previously unimaginable capabilities, has a dark side in that it has opened windows of previously unknown criminal opportunities that not only challenge, but also transcend all physical boundaries, borders, and limitations to detect, punish, and diminish what appears to be a growing social problem of global proportions. The Internet has literally become a fertile breeding ground for an entirely new and unique type of criminal offender hereafter known as the cyber stalker. The cyber stalker is one who uses the Internet as a weapon or

---

[1] Executive Director, Council on Alcohol and Drug Abuse, Allentown, Pennsylvania; Adjunct Professor, Criminal Justice Department Cedar Crest College Allentown, Pennsylvania; 3162 Florian Avenue, Easton, Pennsylvania 18045, United States of America 484-903-9002 Email: crimeNjustice@RCN.com

tool of sorts to prey upon, harass, threaten, and generate fear and trepidation in his or her victims through sophisticated stalking tactics, which for the most part, are largely misunderstood and in some cases, legal.

Despite nearly a decade of prominent criminological research, there is no concise, universally accepted definition of traditional stalking and to make matters worse, there is even less literature available in reference to cyber stalking (McFarlane & Bocij 2003). Consequently, the cyber stalkers' behaviors, patterns, and tactics are largely misunderstood and to a certain extent – unknown (Mustaine & Tewksbury 1999). The term cyber stalking generally refers to the use of the Internet, email, or other electronic communication device to create a criminal level of intimidation, harassment, and fear in one or more victims (Petrocelli 2005; Reno 1999). As mentioned, there is very little known about cyber stalking, but what is accepted is that cyber stalking behaviors can vary from a non-threatening email to a potentially deadly encounter between the stalker and the targeted victim (Hutton & Haantz 2003). The obvious key to distinguishing traditional stalking from cyber stalking is that cyber stalkers rely predominantly on the Internet and other electronic communication devices to harass, threaten, and intimidate their targeted victims. Most cyber stalking behaviors are premeditated, repetitious, and can be quite aggressive in their approach, but border on being illegal under current statutory law in most states (Hutton & Haantz 2003).

Since cyber stalking is largely misunderstood, many incorrectly assume that cyber stalking involves an element of sexual obsession; however, the research findings are not as conclusive in that regard (Mustaine & Tewksbury 1999). Mustaine and Tewksbury (1999) propose that stalking is a criminal offense motivated by interpersonal hostility and aggressive behaviors stemming from power and control issues rather than material gain or sexual obsession. Cyber stalking, like traditional offline stalking, is fueled by rage, power, control, and anger that may have been precipitated by a victim's actions or, in some cases, the victim's inactions. The research suggests that the number of cyber stalking incidents will continue to mount, in part, because the Internet provides a safe haven in which an offender can theoretically hide and conceal one's identity behind a veil of anonymity (Bowker & Gray 2004). With anonymity, an offender can literally pretend to be someone completely different, which is similar to an actor who conjures up a convincing persona to persuade the audience that the actor's guise is, in fact, genuine (Bowker & Gray 2004). The anonymity of the Internet also affords the perpetrator an opportunity to contact virtually anyone with Internet access, at any time, with little fear of being identified and even less fear of being arrested and prosecuted under the current legal system in many jurisdictions (Bowker & Gray 2004).

Part I. Online Cyber stalking vs. Traditional Offline Stalking

To some extent, cyber stalking is fundamentally an extension of traditional stalking in which the offender utilizes a high-tech modus operandi to committing the crime (Petherick 2007). With cyber stalking becoming a growing criminological concern in contemporary society, the offender's behaviors and actions need to be examined in greater depth (Desai & Jaishankar 2007). Bocij (2005) was one of the very first researchers to study the prevalence and impact of cyber stalking. Cyber stalking behaviors are similar to traditional stalking behaviors in many respects; however, cyber stalking, at least from a

criminological and legal perspective, represents an entirely new form of deviant, criminal behavior (Bocij & McFarlane 2002). For one, both offender types, traditional and online, resort to tactics and behaviors that are primarily intended to harass, and in some cases, threaten or intimidate the victim (Petrocelli 2005). As mentioned, traditional stalkers and cyber stalkers will frequently react aggressively when confronted, scorned, rejected, or belittled by a victim (Bocij 2005). The research information suggests that cyber stalkers are demographically more in line with the stereotypical white- collar criminal as opposed to the street level criminal offender. The overwhelming majority of cyber stalker offenders are middle to upper class Caucasian males with stable employment and firmly established ties to the community (Bocij & McFarlane 2002).

Conversely, the research literature also suggests that many cyber stalkers have a prior criminal record, a history of substance abuse, or a personality disorder that directly or partly contributes to, and increases the likelihood of such antisocial behaviors (Hutton & Haantz 2003; Reno, 1999). Although this may be true in some cases, there is very little conclusive evidence to support this claim in all cases (Mustaine & Tewksbury 1999). The figures cited throughout this report are purely speculative based on limited empirical evidence in that the actual numbers or percentages can never be known since most crimes, especially cyber stalking crimes, go unreported or undetected, thereby contributing to the so–called dark figure of crime. In addition, scientific information in relation to cyber stalking is still in its infancy and is therefore, anecdotal. The evidence collected thus far suggests that offender suffers from a personality disorder that may range from an abnormally high level of paranoia to delusional behaviors and thoughts that can consume the offender (Mullen et.al 1999).

As repeatedly mentioned, many of the behaviors displayed by cyber stalkers resemble that of traditional stalkers; however, there are many notable differences that clearly distinguish the former from the latter. One of the most striking similarities is that both offender types are motivated by an insatiable desire and need to have power, control, and influence over the victim (Reno 1999). If left unattended, these actions could conceivably escalate to a potentially volatile physical confrontation between the offender and the victim even though many, including those in law enforcement, perceive cyber stalking to be relatively harmless (Reno 1999).

Traditional stalking behaviors are fairly predictable in that the offender will often follow the victim home, to work, or even to school, thereby making it somewhat effortless for investigators to track, apprehend, arrest, and subsequently prosecute the offender. Further, many stalkers resort to leaving harassing written messages at the victim's home or place of employment and in some cases, the offender will make threatening phone calls that are intended to provoke fear and intimidation in the victim, all of which can often be traced back to the perpetrator with relative ease (Reno 1999). As stated, the aforementioned crimes typically leave a physical trail of evidence behind that will undoubtedly be used to assemble a criminal case against the offender. Another noteworthy comparison between the stalker and the cyber stalker is the distinctively high probability that both offender types had a prior intimate relationship, whether real or perceived, with the victim; however the cyber stalker is more inclined to choose his or her victims at random (Bocij & McFarlane 2003; Reno 1999). According to Reno (1999), nearly 50% of all cyber stalking incidents involved complete strangers who were initially contacted in some perceivably innocent manner via the Internet.

In fact, there has been a considerable increase in the number of stranger cases, particularly with cyber stalkers (Reno 1999). The Internet grants cyber stalkers access to a vast amount of personal information with relative ease (Reno 1999). Information that was once considered private and confidential a few decades ago can easily be accessed through a variety of brokerage websites that cater specifically to individuals innocently searching for friends or loved ones (Reno 1999). Some of these websites are free, but the large majority will charge a small service fee in exchange for a person's name, phone number, address, social security number, date of birth and other confidential identifying information (Reno 1999). The majority of these brokerage sites were established to help people find friends and loved ones of the past, but like anything else, is subject to abuse by those who want to use the service for diabolical reasons.

For example, on July 29, 1999, 21-year old Liam Youens of New Hampshire contacted Docusearch, an Internet-based investigation and information service, and requested information, specifically the date of birth of Amy Lynn Boyer, a 20-year old woman whom Youens had been obsessed with ever since the two attended high school together (Electronic Privacy Information Center 2006). Shortly after receiving the birth dates for several Amy Boyer's, none of which was the Amy Lynn Boyer sought by Youens, Youens, once again, contacted Docusearch for a second time to request Boyer's social security number and employment information, for which Youens was charged a measly $45 (Electronic Privacy Information Center 2006).

On September 8, 1999, Docusearch managed to obtain Boyer's employment information and address by having a subcontractor, Michelle Gambino, place a "pretext" call to Boyer (Electronic Privacy Information Center 2006). Pretexting is the practice of collecting information about a person using false pretenses in which the caller often claims to be someone "official" calling in regard to some proclaimed legitimate purpose (Electronic Privacy Information Center 2006). In this particular case, Gambino "pretended" to be affiliated with Boyer's insurance company in order to attain employment verification information concerning Boyer's workplace address, all of which under the false pretense of facilitating the delivery of a fictitious overpayment refund (Electronic Privacy Information Center 2006). The investigation later revealed that Youens paid Docusearch $109 for this information. On October 15, 1999, Youens, armed with a handgun and a map to Boyer's place of employment, drove to the dentist's office in Nashua, New Hampshire where Boyer worked and fatally shot her – 11 times – as she left work, before turning the gun on himself in a senseless act that was quickly ruled a murder-suicide (Spencer 2000).

To make matters worse, the investigation into Boyer's murder discovered that Youens had constructed and maintained a website titled, *Amy Boyer,* for nearly two years prior to the murder, which contained explicit details of how he had stalked her for years, how he felt about her, and more alarmingly, how he planned to kill her (Spencer 2000). On the website, Youens explained how he had fallen in love with Boyer in the eighth grade, how she had rejected him in high school, and in response to the rejection, a detailed chronicle of why and how she must die (Spencer). An excerpt from the webpage reads, "*When she gets in, I'll drive up to the car blocking her in, window to window, then I'll shoot her with my Glock*," which is tragically the way it occurred on October 15, 1999 (Spencer 2000). How could Youens' rambling messages regarding his intentions to kill Amy Boyer

go unnoticed? The existing laws, as will be seen, are virtually meaningless when the cyber stalkers are across states lines, especially when threats are only implied.

In response to Boyer's death, her mother and stepfather (*Helen and Tim Remsburg*) filed a wrongful death suit against Docusearch and the investigators that the agency subcontracted with to obtain Boyer's personal information (Electronic Privacy Information Center 2006). The suit claimed an invasion of privacy through intrusion upon seclusion; invasion of privacy through commercial appropriation of private information; violation of the Fair Credit Reporting Act; and violation of the New Hampshire Consumer Protection Act (Electronic Privacy Information Center). The Electronic Information Privacy Center filed an amicus brief on behalf of the Remsburg's arguing that Docusearch should be held liable under all the aforementioned claims.

In addition to the people-search websites via Google and other popular search engines, the Internet is host to a number of sites that specifically promote retaliation and revenge, which is, in essence, a cyber stalker's dream (Bocij 2005). For instance, cyber stalkers who wish to send anonymous letters or emails can do so through the "payback" website at www.thepayback.com , a site that purposely conceals and protects the sender's name and personal information (Bocij 2005). There are also a number of radical extremist sites, including the Avenger's page, a site that encourages visitors to seek revenge and, in some instances, incite violence (Bocij 2005).

Case in point, a Pennsylvania State Trooper was recently arrested for posting five nude photographs of his former wife on a bondage and sadomasochistic website apparently in order to seek revenge for a failed marriage. According to Christine Pittaro (2007), the Crime Victim / Witness Advocate for the District Attorney's Office of Northampton County, Pennsylvania, Heller had worked as a trooper for approximately 14 years – up until the date of his arrest. In addition to creating a profile in his wife's name and posting the nude photographs, Heller also posted his wife's occupation as a schoolteacher and date of birth on the bondage website (Pittaro 2007). A forensic examination of Heller's laptop computer revealed that the laptop had been used to post five of the 18 nude photographs of his ex-wife that were taken when the two were initially married (Iannace 2007).

The forensic examination, which was performed by State Trooper Paul Iannace, determined that Heller, posing as his ex-wife, posted explicit messages on the website-soliciting viewers to contact her to engage in violent sexual acts (2007). This particular cyber stalking offense was unearthed after one of the website's visitors decided to contact Heller's ex-wife at her place of employment (Iannace 2007). Heller subsequently pleaded guilty to harassment for placing the images on the bondage site and agreed to quit the Pennsylvania State Police in light of the criminal charges lodged against him (Iannace 2007). According to Assistant District Attorney Patricia Broscious of Northampton County, Pennsylvania, such cases of cyber stalking are difficult to prosecute based on the manner in which many of the statutes are currently written (Iannace 2007).

One obvious difference between traditional stalking and cyber stalking is the geographic proximity between the offender and the victim. In a traditional stalking case, the offender and victim often live or work within relatively close proximity of one another whereas cyber stalkers could literally be harassing the victim from the house across the street or from a coffee shop in another state, or even another country for that matter (Reno 1999). One of the many advantages that cyber stalkers have over the traditional stalker is that these offenders typically have a high level of computer proficiency and aptitude, essential skills that allow the stalker to take crucial steps toward avoiding

detection (Hutton & Haantz 2003). As stated, the anonymity of the Internet allows the cyber stalker to easily conceal one's identity through a variety of inexpensive and simple tactics. For instance, cyber stalkers can connect to several different Internet service providers, thereby creating a number of screen names, which will make it nearly impossible to track the origin of the emails (Reno 1999).

As mentioned, there is rarely any physical contact between the cyber stalker and the victim, therefore, most police officers minimize the seriousness of such harassment and simply dismiss the victim's fears as nuisance complaints (Reno 1999). However, cyber stalking can be just as threatening and as frightening as being followed and watched by a traditional stalker in one's neighborhood (Reno 1999). Cyber stalking behaviors like those of sexual offenders like the peeping Tom voyeur may simply be a prelude to other dangerous disturbed behaviors, some of which may end in violence (Bocij 2005; Reno 1999). The level of dangerousness is elevated further if the offender has a criminal record, a history of substance abuse, or a psychological disorder, which predisposes the offender to violence (Bocij 2005).

Even though most stalkers act alone, the Internet has made it much easier for cyber stalkers to conspire and encourage third parties to harass victims in chat rooms, discussion boards, and within Internet public forums (Reno 1999). In fact, researchers have coined the term, stalking by proxy, to describe the process in which cyber stalkers encourage others such as family members and friends to aid in harassing the victim (Bocij & McFarlane 2003). Some cyber stalkers have even been known to hire private investigators to follow and report on the victim's daily activities and whereabouts (Bocij & McFarlane 2003) Private investigators can also be used to obtain additional personal information on the victim that may not be readily available on the Internet as in the case of Amy Lynn Boyer (Bocij & McFarlane 2003).

Part II. The Internet as a Medium for Online Predatory Behavior

The Internet is particularly appealing to cyber stalkers and other online predators, simply because many are drawn to its relatively inexpensive cost, ease of use, and as previously mentioned, its anonymity in seeking out victims and avoiding detection (Reno 1999). Cyber stalking behaviors are often misunderstood and confused with other online predatory behaviors, including those of sexual offenders who seek out children purely for sexual gratification (Dombrowski et.al 2004).

As mentioned, not all cyber stalking incidents are motivated by sexual obsession. However, one cannot discount the fact that the Internet has become a virtual playground for sex offenders because it provides predators with easy access to literally tens of thousands of children and presents a completely new and unique way to groom a child from afar (Dombrowski et.al 2004). This is particularly frightening considering that nearly 30 million children have regular access to the Internet in the United States alone with little to no parental supervision (Dombrowski et.al 2004). Adolescents, in particular, tend to be the most vulnerable group in light of the group's collective sexual curiosity and continuous exploration with pornography websites (Dombrowski et.al 2004). There are number of websites such as www.myspace.com that allow adolescents to post and exchange personal and often sensitive information about one another. What these adolescents fail to recognize or accept is that this information is publicly accessible to

anyone who visits the site, including those who prey upon children (Dombrowski et.al 2004). Myspace and other social networking websites have security measures in place, but there is no foolproof way to truly secure access to a potential smorgasbord of victims given today's computer savvy offenders.

Prevalence

As of February 2002, 54% of all Americans accessed the Internet on a regular, consistent basis and more than half of all households in the United States had contracted with an Internet service provider at home (Schneider 2003). In the United States alone, more than 80 million adults and 10 million children have access to the Internet whether it be at home, work, school, or one of the many emerging wireless provider locations (Reno 1999). As with any crime, there is no practical, truly scientific way of predicting with 100% accuracy the prevalence of cyber stalking in the United States (Reno 1999). To this writer's surprise, criminologists and other researchers have only recently begun to gather information on cyber stalking behaviors, trends, and patterns (Reno 1999). Nevertheless, the most recent findings have unveiled some fascinating information, but these findings should be approached with a degree of caution since the information has only been compiled and evaluated on a relatively small scale (Reno 1999). The anecdotal evidence presented thus far suggests that cyber stalking is a serious societal problem that warrants further review and attention, particularly because cyber stalking, by all measurable accounts, is on the rise (Reno 1999).

In order to gain a true understanding and practical insight into the extent of cyber stalking, it would be best to study the behaviors associated with traditional stalking offenders since many of those same behaviors overlap with those of cyber stalkers (Reno 1999). Since California leads the nation in the number of cyber stalking cases, it would be best for researchers to make California the focal point for future research (Reno 1999). This approach would be similar to that taken by sociologists in the 1920's who were interested in studying the relationship between immigration demographics and Chicago's rising crime rates, a movement which eventually led to the birth of the Chicago School of Criminology (Barkan 2006). What makes California so unique? There must be a logical reason to explain why the majority of cyber stalkers emanate from California and it needs to be explored.

Email

The research findings strongly suggest that cyber stalkers use email as the primary means to harass and threaten victims, far more than any other electronic communication device (Petrocelli 2005). Emailing allows an offender to repeatedly transmit harassing, threatening, hateful, or obscene messages, including pictures, videos, or audio (Petrocelli 2005). In rare instances, cyber stalkers were known to purposely transmit electronic files that contain a hidden computer virus, which is intended to damage the victim's electronic files and spread the virus to others in the victim's "address" book (Hutton & Haantz 2003). In some cases, cyber stalkers use the victim's email address and other personal information to subscribe to or purchase books, magazines, or other Internet services without the victim's knowledge or consent (Hutton & Haantz 2003).

As such, revenge and retaliation appear to be the key components of cyber stalking (Hutton & Haantz 2003). As noted, cyber stalkers have been known to send the victim's private information to websites that cater specifically to pornography in the hopes that the

site will continuously inundate the victim with obscene email messages and pop-ups as noted in the Heller case that was mentioned earlier in this report (Hutton & Haantz 2003). A clever cyber stalker will frequently use computer programs that are specifically designed to repeatedly send out enormous amounts of explicit emails at regular or random intervals (Reno 1999). Moreover, this offender is also likely to use anonymous re-mailers that make it virtually impossible for Internet service providers, law enforcement, or victims to trace the emails' point of origin (Reno 1999).

According to Ogilvie (2000), cyber stalking patterns often replicate that of traditional stalking behaviors in that the intent is often to establish a relationship or mend a previously established relationship, whether real or perceived. The introduction of spy ware has enabled cyber stalkers to purchase inexpensive software that was created specifically to notify the perpetrator whenever the victim is online (Petrocelli 2005). All one needs, in most cases, is merely the victim's screen name (Petrocelli 2005). The victim could conceivably block such messages, but it is highly likely the computer savvy cyber stalker will eventually find a way around the block. Victims are then forced to change Internet providers or adopt another screen name.

Cyber stalkers often enter discussion boards, chat rooms, and the like, for attention or mere companionship (Stephens 1995). Once contact has been initiated, the cyber stalker will continue to befriend the victim. In many cases, the cyber stalker perceives that a "relationship" exists when one does not. In other words, the cyber stalker truly believes that a relationship exists even though the victim may have innocently responded to an offender's question in a chat room or discussion board (Stephens 1995). However, if the offender believes that the relationship has been jeopardized in any way, the cyber stalker may launch into a full-fledged campaign to ruin the victim's reputation, financial credit, or personal identity (Stephens 1995).

Discussion forums are typically a place for Internet users to post opinions and comments on one or more subjects. However, discussion boards can also be a place for cyber stalkers to post harmful, negative personal information about the victim, including the victim's name, address, phone number, email address, and other private information (Petrocelli 2005). The term *cybersmearing* is used to refer to the posting of embarrassing or humiliating rumors about the victim in a chat room, newsgroup, or bulletin board (Bocij & McFarlane 2003). The most common form of cybersmearing is the posting of false sexual innuendos about the victim (Petrocelli 2005). This online verbal abuse can also take the form of chat harassment or what is commonly referred to as *flaming,* in the cyber world, in which the victim is belittled or demeaned in a live public forum (The National Center for Victims of Crime, Cyber stalking 2004).

Part III. Typology, Etiology of Cyber stalking and Victims

a. Typology of Cyber stalkers

McFarlane and Bocij (2005) have conducted one of the most exhaustive studies on cyber stalkers and stalking victims. Four distinct types of cyber stalkers emerged from the data. There have been other studies, but the others pale in comparison to this particular study in this writer's opinion. According to McFarlane and Bocij, the four types include the Vindictive Cyber stalker, the Composed Cyber stalker, The Intimate Cyber stalker, and the Collective Cyber stalker (McFarlane & Bocij 2005).

According to McFarlane and Bocij (2005), the Vindictive Cyber stalker is one that is particularly malicious. Offenders in this group were found to threaten and harass victims far more often than the other three groups (McFarlane & Bocij 2005). This group was more likely to employ a number of spiteful tactics that were intended to continuously harass victims through excessive spamming, email bombing, and identity theft (McFarlane & Bocij 2005). Vindictive Cyber stalkers were the only group of the four to purposely use *Trojans* to access the victim's computer and deliberately infect the computer with a destructive virus (McFarlane & Bocij 2005). The group's computer skills and proficiency ranged from medium to high and there was some indication that mental illness was present based on the bizarre, disturbing content that was often transmitted to victims (McFarlane & Bocij 2005). This writer would place Liam Youens in this particular category based on Youens' bizarre behaviors and obsession with stalking and eventually murdering Amy Lynn Boyer.

The Composed Cyber stalker targeted victims in calm, poised, and unruffled manner (McFarlane & Bocij 2005). The primary purpose of the harassment was to cause constant distress in the victim through a variety of threatening behaviors (McFarlane & Bocij 2005). This writer would place former State Trooper Luke Heller in this particular category based mostly on media reports of the crime and interviews with those intimately familiar with the case. With the Intimate Cyber stalker, the primary objective was to establish a relationship with an intended target that was based more on infatuation and obsession (McFarlane & Bocij 2005). This group was the most diverse in that some were once personally involved with the victim or were simply infatuated with a targeted individual (McFarlane & Bocij 2005). Collective Cyber stalkers as the name implies consists of two or more individuals who pursue the same victim (McFarlane & Bocij 2005). This group's computer skills were exceptionally high when compared to the other three types of cyber stalkers (McFarlane & Bocij 2005).

b. Etiology of Stalking
Possible Psychological Explanation

As mentioned earlier, one commonly held myth is that cyber stalkers commit such crimes because of some mental abnormality (Bocij & McFarlane 2003). Granted, most of the literature findings to date suggest that this may be true; however, some of the studies, with the exception of those pertaining to Bocij and McFarlane (2003) suggest that stalkers suffer from de *Clerambault's syndrome*, an erotomanic type of delusional disorder that can be found in the DSM-IV (Dressing, Henn, & Gass 2002). This syndrome is used to explain the obsessive and compulsive behaviors of those individuals who truly believe that they are in an intimate relationship with the victim (Dressing, Henn, & Gass 2002). Other studies suggest that stalking is not the result of a mental disorder but rather a behavioral disorder that stems from various psychopathological conditions, including paranoid and delusional disorders (Dressing, Henn, & Gass 2002). However, this is not always the case with cyber stalkers. Cyber stalkers tend to be emotionally distant loners who simply want to seek the attention and companionship of another (Hutton & Haantz 2003). The problem lies in the fact that these individuals often become obsessed or infatuated with the victim, but the victim does not reciprocate those same feelings and perceptions about the relationship (Hutton & Haantz 2003).

Social Learning Theory

What is known is that both online and offline stalkers are driven by an underlying desire to exert some type of power and control over the targeted victim (Reno 1999). If one were to approach cyber stalking from a behaviorist's perspective, one would start by citing the early research of B.F. Skinner and others who drew from the psychological research concerning classical and operant conditioning (Barkan 2006). In classical conditioning, the frequency of an exhibited behavior is often contingent upon the amount of external positive reinforcement received (Barkan 2006). With operant conditioning, certain behaviors are often repeated when rewarded and therefore, positively reinforced (Barkan 2006). If the same behavior is met with a negative response, the behavior is likely to diminish since a reward was not present (Barkan 2006). If a stalker makes contact with the victim and victim engages in a discussion whether positive or negative, the stalker is likely to repeat the action. In other words, it may be best to ignore the stalker rather than offer a negative response. Exhibitionists often display similar behaviors. Exposing one's genitals to an innocent victim is likely to illicit a response, albeit a shocked response. Even though the response is typically negative, the behavior is still reinforced and therefore sought in all subsequent incidents.

Rational Choice Theory

Rational choice theory suggests that individuals, which in this case would be cyber stalkers, freely choose to commit a crime after weighing the prospective rewards against the potential risks (Barkan 2006). Routine activities theory can be integrated with rational choice theory because routine activities theory assumes that individuals will commit a crime if there is a motivated offender, suitable target, and absence of guardians capable of preventing the offense from successful commission (Barkan 2006; Mustaine & Tewksbury 1999). In other words, the cyber stalker, as a motivated offender, will seek out and stalk a victim, a suitable target, in the absence of capable guardianship, which, in this situation, is through the anonymity of the Internet that provides protection against detection. According to Mustaine and Tewksbury (1999), women may be suitable targets because cyber stalking victimization is not yet taken seriously by society nor has it received the attention it deserves from the criminal justice system. Stalking via the Internet allows the offender to stalk at a relatively remote distance, yet the offense can still inflict the same type of fear and harassment in the victim as if the victim were in a direct face-to-face encounter with an offender.

Since rational choice theory assumes that cyber stalkers will calculate the risks before committing a crime, it also assumes that such behaviors could be deterred if the risks were certain and the punishment were severe (Barkan 2006). At the present time, there is no true deterrent against such behaviors. The risk of detection is low and even if the cyber stalker's identity is revealed, the threat of being arrested, prosecuted, and found guilty of such crimes is exceptionally low; thereby making cyber stalking a relatively safe and attractive crime to commit. Based on what has been presented, it appears that routine activities theory, at least as an outgrowth of rational choice theory, can have a significant amount of explanatory potential in future criminological studies.

Treatment

Rosenfeld (2003) was the first to conduct an empirical study on the relationship between stalkers and recidivism. Rosenfeld's (2003) findings, although limited to traditional stalkers, determined that roughly 50% of those studied re-offended. The strongest predictors of recidivism include the presence of a personality disorder, particularly those that involve antisocial, borderline, or narcissistic behaviors, which are collectively referred to as "Cluster B" personality disorders (Rosenfeld 2003). The combination of a personality disorder and a history of substance abuse raised the risk of re-offending even higher (Rosenfeld 2003). This is consistent with the findings associated with other criminal offender groups. Based on experience, those offenders with a history of mental illness and substance abuse have a higher than normal probability of re-offending.

Unfortunately, there are several obstacles to treating this disorder. First, finding a qualified mental health professional that acknowledges this condition and specializes in this type of treatment may be a cumbersome task to accomplish (King 1996). The literature on cyber stalking is scarce at best and the studies that have been done have been based on comparatively small sample populations. From what has been researched, it is doubtful that mental health professionals even have a general understanding of cyber stalking behaviors and are less likely to know how to approach and treat this particular offender. The Internet is one of the most resourceful advancements in technology to have ever been created by humankind, but it also has a malevolent side to it that cannot be discounted. Clinicians have only recently begun to understand the dangers associated with the Internet.

c. Cyber stalking Victims

Like most traditional crimes, cyber stalking knows no boundaries. Anyone can become a stalking victim, whether it is random or predicated on poor judgment when one releases personal information on the Internet. Even though most of the evidence is anecdotal, it strongly suggests that the majority of cyber stalkers are men and the victims are women; however, there have been several highly publicized cases of females stalking men and same-sex stalking (Reno 1999). Unlike male stalkers, Female stalkers are more inclined to stalk and harass ex-partners and less likely to stalk strangers (Purcell, Pathe, & Mullen 2001). Female stalkers are also more likely to target other females in the hopes of establishing an intimate relationship with the victim (Purcell, Pathe, & Mullen 2001). According to Purcell, Pathe, and Mullen (2001), female stalkers are very similar to males in regard to demographic profiles and psychiatric status, however males are more likely to have a history of criminal offending or substance abuse (Purcell, Pathe, & Mullen 2001).

As noted, virtually anyone can become a victim, but certain demographic groups are more at-risk than others such as women, juveniles, newcomers to the internet, and other particularly vulnerable groups (Hutton & Haantz 2003). In a 2002 study conducted by the online victim advocacy group, *Working to Halt Online Abuse*, 71% of cyber stalking victims were women and 59% of that group had some type of previous relationship with the stalker (Hutton & Haantz 2003). A prior relationship, whether real or perceived, seems to be the catalyst for cyber stalking, particularly when the victim attempts to end the relationship (Reno 1999).

Interestingly, a 2001 research study concluded that 61% of the cyber stalking victims were Caucasian followed by Asians with 3.9% and African Americans with 1.6%

(McFarlane & Bocij 2003). One should approach these findings with a degree of caution since the survey data was confined to the United States with only a minimal number of respondents (McFarlane & Bocij 2003). However, several follow-up studies have revealed similar findings in that the majority of victims are Caucasian women between the ages of 18 and 30 (McFarlane & Bocij 2003).

Nearly four out of five victims are females and females are eight times as likely to be the stalking victims of ex-partners or acquaintances (Hutton & Haantz 2003). Due to the different levels of online harassment, some victims may not report the harassment to law enforcement for one reason or another (Hutton & Haantz 2003). It has been speculated that the majority of cyber stalking victims do not report being victimized for one of two reasons. First, the victim may feel that the behavior is not serious enough to warrant the attention of the police or secondly, the victim does not believe that law enforcement will take the matter seriously (Reno 1999). Sadly, when a victim does report a cyber stalking incident to law enforcement, many law enforcement agencies simply advise the victim to come back if the perpetrator confronts them or makes a threatening statement offline (Reno 1999). As of this writing, there are only a small number of online victim advocacy groups available to assist, support, and advise cyber stalking victims (Pittaro 2007).

In response to being stalked, some cyber stalking victims may experience abrupt changes in sleep and eating patterns, nightmares, hyper vigilence, anxiety, helplessness, and fear for safety (The National Center for Victims of Crime, Cyber stalking 2004). Hyper vigilence is often associated with Posttraumatic Stress Disorder (PTSD)to describe a symptom whereby the victim, when in a state of fear, lashes out inappropriately through aggressive and, at times, violent behavior (Bocij 2005).

Very rarely do brief episodes of stalking cause distress in the victim; however, there have been a number of stalking incidents that have extended for weeks, months, or even years (Mullen 2003). The frequency of such communication greatly increases the risk of a potential physical assault (Mullen 2003). Victimization may also lead to vandalism but not necessarily vandalism in the traditional sense of the term. Vandalism is typically associated with traditional stalking; however, vandalism can also take place in cyberspace as well. For instance, vandalism may be used to damage the victim's personal computer data with the assistance of a computer virus or Trojan horse program as mentioned earlier (Bocij & McFarlane 2003). As mentioned, there are a number of Internet websites out there in cyberspace that will happily provide interested parties with information on a victim (Reno 1999).

Part IV. Legal and Social Issues of Cyber stalking

Unique Challenges for Law Enforcement

According to Petrocelli (2005), cyber stalking crimes present a unique challenge to law enforcement, particularly to those departments that lack the expertise or resources to investigate and prosecute cyber stalkers. Local law enforcement is at a particular disadvantage as result of jurisdictional limitations (Petrocelli 2005). For example, a stalker may be in another city, county, state, or even country, thereby making it difficult if not entirely impossible to investigate and prosecute (Petrocelli 2005).The anonymity of the Internet also places the cyber stalker in a truly advantageous position over law

enforcement investigators (Reno, 1999). Petrocelli (2005) claims that some victims went to the police for help, but were ill advised to, simply turn the computer off and that the harassment would stop. Clearly, this is an inappropriate response and quite unrealistic considering most individuals have come to rely on the Internet – both professionally and personally. Thankfully, some of the larger metropolitan police departments such as Los Angeles and New York have created computer crime units that deal specifically with computer-related crimes (Petrocelli 2005). In response to the growing number of cyber stalking cases, the Federal Bureau of Investigation (FBI) has created a number of Computer Crime Squads in which agents are schooled and experienced in cyber stalking investigations (Petrocelli 2005). The FBI has, in turn offered to assist local and state law enforcement in tracking and prosecuting cyber stalkers (Petrocelli 2005).

Most cyber stalkers have turned to cable service providers as the preferred Internet service provider because the Internet connection speeds are far faster and reliable than the antiquated dial-up connections (Reno 1999). One apparent obstacle in investigating an alleged cyber stalking incident is that the *Cable Communications Policy Act of 1984* requires law enforcement agencies to obtain a court order if the request is for personal information on a cable subscriber (Reno 1999). To complicate matters further, the cable company is required to notify the suspect, in advance, that law enforcement officials have requested an inquiry into the suspect's records (Reno 1999). The warning could conceivably jeopardize the entire investigation if a suspect attempts to destroy all evidence that is even remotely connected to the alleged cyber stalking incident.

Regrettably, there are a number of websites that allow users to set up free email accounts with little personal information. Even though the site requires the individual to list identifying information, it rarely authenticates that the personal information provided is accurate, thereby hindering law enforcement efforts further (Reno, 1999). Moreover, a number of email servers will purposefully remove identifying data for a small fee making it extremely difficult for law enforcement to trace the account (Reno 1999). Many cyber stalkers who subscribe to such a service will pay with either a money order or some other non-traceable form of payment to avoid detection (Reno 1999).

Anti-Stalking Legislation in the United States

To date, all 50 states and the District of Columbia have adopted criminal stalking statutes (Reno 1999). As of 2005, 44 states have enacted cyber stalking laws within existing stalking or harassment laws (National Conference of State Legislatures 2006). According to Reno, Title 18 U.S.C. 875(c) makes it a federal crime to transmit any interstate or foreign commerce containing a threat that is intended to injure another person. The penalty for violating the law is a prison sentence punishable up to five years and may include a fine of up to $250,000 (Reno 1999). One glaring problem with the federal law is that the communication must specifically include a direct rather than implicit threat to harm another. Cyber stalking communication does not always include a specific message in which the perpetrator threatens to harm the victim.

The basic foundation of criminal law requires the following two elements to be present for a crime to have been committed: *actus reus* and *mens rea* (Dennison & Thomson 2002). *Actus reus* or the "act" requires that certain behaviors take place and *mens rea*, the guilty mind, requires that the offender intended to cause harm (Dennison & Thomson 2002). A third element requires that there be a victim (Dennison & Thomson 2002). Establishing actus reus is not as difficult as establishing mens rea whereby the state

(prosecution) must prove that the perpetrator intended to cause harm (Dennison & Thomson 2002). Dennison & Thomson found that it was easier to prove intent in ex-intimate relationships than it was in stranger or acquaintance cases (2002).

In certain situations, cyber stalking may be prosecuted under 47 U.S.C. 223, a federal statute that makes it a crime to use a telephone or any other communication device to harass or threaten any person (Reno 1999). The statute is somewhat easier to apply to cyber stalking cases because it includes both harassment and threats unlike that in Title 18 U.S.C. 875(c) (Reno 1999). Fortunately, harassment is such a vague term that it includes virtually any behavior that may be interpreted as a nuisance. Even though it does not mention cyber stalking specifically by name, the *Interstate Stalking Act of 1996* makes it a crime for anyone to travel from one state to another with the intent to injure or harass that person (Reno 1999). The problem with enforcing this law lies in the language used in the legislation whereby the offender must physically travel across the state line, which clearly rules out most cases of Internet harassment (Reno 1999). In addition to what has been cited, *The Violence Against Women Act of 2000* made cyber stalking part of the federal interstate stalking statute, a federal crime (The National Center for Victims of Crime, Cyber stalking 2004).

Cyber stalking State Statutes

According to Reno (1999), the first traditional stalking law was enacted slightly more than a decade ago in 1990 when California passed a law making stalking a criminal offense. As in the federal laws that have been cited in this report, most traditional stalking laws require that the perpetrator make a direct threat to injure or in some way – harm the victim or victims (Reno 1999). However, some state laws will prosecute an offender if the behavior or conduct displayed constitutes an implied threat (Reno 1999). Since most state laws require a direct threat of harm to the victim, many perpetrators can avoid arrest and prosecution in the absence of a direct threat. In other words, the harassment can continue as long as the stalker does not directly threaten the victim or the victim's family with bodily injury, which appears to be the case in the Heller example that was cited earlier (Reno 1999). In addition to criminal sanctions, some states allow victims to file a civil suit against the harasser for injuries, including defamation, slander, pain and suffering, or lost income to name a few (Hutton & Haantz 2003).

Societal Intervention and Prevention

Law enforcement officials have suggested that to prevent being a victim, people choose screen names that are gender and age ambiguous and if possible, avoid posting personal information in web profiles (Petrocelli 2005). Most importantly, be extremely cautious when meeting with an individual that was met online (Petrocelli 2005). Petrocelli (2005) suggests that if a meeting is to take place that it is done in a public location and it is strongly advisable to bring a friend along. To aid in the investigation, cyber stalking victims should be advised to inform the perpetrator that the communication is unwanted and should cease immediately (Petrocelli 2005). It is also advisable to save all unaltered and unedited communication from the perpetrator that could be used as prosecutorial evidence (Petrocelli 2005). Establishing a pattern of harassment is paramount to the investigation and the success of prosecution (Hutton & Haantz 2005).

Victims can also purchase software to block, squelch, or ignore unwanted electronic communication and it would be advisable to contact one's Internet Service Provider since most ISPs have established policies in the online agreement prohibiting such abuse of services (Hutton & Haantz 2003). The ISP can immediately terminate the offender's service for violating this policy without fear of legal recourse by the offender (Hutton & Haantz 2003). However, the reality of the situation is that most ISPs have concentrated more on helping its customers avoid spam, unwanted pop-ups, and virus protection rather than protecting against online harassment (Hutton & Haantz 2003). The problem lies in the fact that complaint procedures are often hard to locate and somewhat vague, resulting in an inadequate follow-up on such complaints (Reno 1999).Victims may also consult one of the many victim advocacy groups such as Working to Halt Online Abuse or CyberAngels, for assistance, support, and advice on cyber stalking (Petrocelli 2005). According to McFarlane and Bocij (2003), CyberAngels is arguably the best-known internet safety agency and one of the largest victim advocacy groups.

Part V. Discussion and Conclusion

The literature on cyber stalking is still in its infancy; however, the incidence of cyber stalking is expected to increase as the Internet becomes even more popular than it is today, especially amongst society's youth (Hutton & Haantz 2003). Simply stated, much of modern life cannot be performed as effectively without continuous access to the World Wide Web (Hutton & Haantz 2003). Even though law enforcement is faced with a series of obstacles, there is hope. Law enforcement at the federal, state, and local level must unite, share, and disseminate intelligence information. With proper training and guidance, law enforcement investigators can often trace, with some accuracy, an electronic trail that has been left behind by the cyber stalker (Reno 1999). Metaphorically speaking, an electronic trail is the equivalent of burglar who leaves behind a fingerprint at the crime scene (Reno 1999). With a little work, the electronic trail can often be traced back to its initial point of origin.

In the interim, law enforcement can resort to investigative strategies and tactics that have proven effective in traditional stalking situations (Reno 1999). Former Attorney General Janet Reno (1999) suggested that law enforcement refer to an annual report generated by the Attorney General's Office to Congress entitled, "*Stalking and Domestic Violence*" for additional insight into stalking behaviors. Additionally, it is strongly suggested that law enforcement form a cooperative partnership with ISPs since both are ultimately working towards the same goal, eradicating online harassment.

Still, not all the law enforcement training and support in the world can replace good ole fashioned education by informing citizens of the dangers associated with the Internet. Online harassment is unfortunately only one of the many detrimental components to the Internet. Former Attorney General Janet Reno (1999) recommended that states review existing stalking statutes to include a section on cyber stalking. Pennsylvania is one of a handful of states that does not have a separate statute or subsection to address cyber stalking, therefore making it incredibly difficult to prosecute such offenses.

Contrary to critics of cyber stalking literature, cyber stalking is a growing problem that transcends international boundaries (Bocij & McFarlane 2002). Granted, the inaccuracies stem from the media's false depiction of cyber stalking as a problem of

epidemic proportion (Bocij & McFarlanem2002). However, the number of cases is increasing and it expected to continue to rise over the next decade (Bocij & McFarlane 2002). In other words, the attention that cyber stalking has recently received is warranted and genuine and worthy of further criminological research (Bocij & McFarlane 2002).

References

Barkan, S. (2006). *Criminology: A sociological understanding*. 3rd ed. Upper Saddle River, NJ: Prentice Hall.

Bocij, P. (2005). Reactive stalking: A new perspective on victimization. *The British Journal of Forensic Practice*, 7(1), 23-45.

Bocij, P., & McFarlane, L. (2003). Seven fallacies about cyber stalking. *Prison Service Journal*, *149*(1), 37-42.

Bocij, P., & McFarlane, L. (2002). Cyber stalking: Genuine problem or public hysteria?. *Prison Services Journal*, *140*(1), 32-35.

Bowker, A., & Gray, M. (2004). An introduction to the supervision of the cybersex offender. *Federal Probation*, *68*(3), 3-9.

Broscious, P. (2007). Personal communication obtained on May 11, 2007.

Dennison, S. M., & Thomson, D. M. (2002). Identifying stalking: The relevance of intent in commonsense reasoning. *Law and Human Behavior*, *26*(5), 543-558.

Desai, M., & Jaishankar, K. (February 2007). Cyber stalking victimization of girl students: An empirical study. *Paper presented at the second International and Sixth biennial Conference of the Indian Society of Victimology at Chennai, India* (pp. 1-23).

Dombrowski, S. C., LeMasney, J. W., Ahia, E. C., & Dickson S. A. (2004). Protecting children from online sexual predators: Technological, psychoeducational, and legal considerations. *Professional Psychology*, *35*(1), 65-73.

Dressing, H., Henn, F. A., & Gass P. (2002). Stalking behavior: An overview of the problem and a case report of male-to-male stalking during delusional disorder. *Psychopathology*, *35*(5), 313-319.

Electronic Privacy Information Center, (2006, June 15). The Amy Boyer case. Retrieved May 7, 2007, from Electronic Privacy Information Center Web site: http://www.epic.org/privacy/boyer/

Hutton, S. (2003). Cyber stalking. Retrieved Feb. 18, 2006, from National White Collar Crime Center Web site: http://www.nw3c.org.

Iannace, P. (2007). Personal communication obtained on May 11, 2007.

Jaishankar, K., & Uma Sankary, V. (2005). Cyber stalking: A global menace in the information   super highway. *ERCES Online Quarterly Review, 2(3)*, Retrieved May 7, 2007, from http://www.erces.com/journal/articles/archives/volume2/v03/v02.htm.

King, S. A. (1996). *Is the Internet Addictive, or Are Addicts Using the Internet?* Retrieved February 18, 2006, from Web site: http://webpages.charter.net/stormking/iad.html

McFarlane, L., & Bocij, P. (2005). An exploration of predatory behaviour in cyberspace: Towards a typology of cyber stalkers. *First Monday*, 8. Retrieved Feb 18, 2006, from http://firstmonday.org/issues/issues8_9/mcfarlane/index.html.

McFarlane, L., & Bocij, P. (2003). Cyber stalking: defining the invasion of cyberspace. *Forensic Update*, *1*(72), 18-22.

Mullen, P. E. (2003). Multiple classifications of stalkers and stalking behavior available to clinicians. *Psychiatric Annals*, *33*(10), 650.

Mullen, P. E., Pathe M., Purcell R., and Stuart, G. W. (1999). Study of stalkers. *The American Journal of Psychiatry*, *156*(8), 1244-1250.

Mustaine, E. E., & Tewksbury, R. (1999). A routine activity theory explanation for women's stalking victimizations. *Violence Against Women*, *5*(1), 43-62.

National Conference of State Legislatures, (2006). State computer harassment or "cyber stalking" laws. Retrieved Feb. 18, 2006, from National Congress of State Legislatures Web site: http://www.ncsl.org/programs/lis/cip/stalk99.htm.

National Conference of State Legislatures, (2001, February). Public internet / private lives. Retrieved May 7, 2007, from National Conference of State Legislatures Web site: http://www.ncsl.org/programs/pubs/201net.htm

Ogilvie, E. (2000). Cyber stalking. Retrieved Feb. 18, 2006, from Australian Institute of Criminology Web site: http://www.aic.gov.au/publications/tandi/tandi66.html.

Petherick, W. (2007). Cyber stalking. Retrieved May 9, 2007, from CrimeLibrary.com Web site: http://www.crimelibrary.com/criminology/cyberstalking/

Petrocelli, J. (2005). Cyber stalking. *Law & Order*, *53*(12), 56-58.

Pittaro, C. (2007). Personal communication obtained on May 14, 2007.

Purcell, R., Pathe, M., & Mullen P. E. (2001). A study of women who stalk. *The American Journal of Psychiatry*, *158*(12), 2056-2061.

Rosenfeld, B. (2003). Recidivism in stalking and obsessional harassment. *Law and Human Behavior*, *27*(3), 251–265.

Reno, J. (1999). 1999 report on cyber stalking: A new challenge for law enforcement and industry. Retrieved Feb. 18, 2006, from United States Department of Justice Web site: http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

Schneider, J. P. (2003). The impact of compulsive cybersex behaviours on the family. *Sexual and Relationship Therapy*, *18*(3), 1468-1479.

Spencer, S. (2000, March 23). An online tragedy. Retrieved May 7, 2007, from CBSNews.com Web site: http://www.cbsnews.com/stories/2000/03/23/48hours/printable175556.shtml

Stephens, G. (1995). Crime in cyberspace. *The Futurist*, *29*(5), 24-29.

The National Center for Victims of Crime, (2004). Cyber stalking. Retrieved Feb. 18, 2006, from The National Center for Victims of Crime Web site: http://www.ncvc.org/ncvc/Print.aspx?PrintableZoneID=Cell_3&PrintableVertionID=WP_P.htm.

The National Center for Victims of Crime, (2004). Stalking fact sheet. Retrieved Feb. 18, 2006, from The National Center for Victims of Crime Web site: http://www.ncvc.org/src/AGP.net/components/Documentviewer/Download.aspXnz?DocumentID=41223.

Working to Halt Online Abuse (WHOA), (2004). Locations of victims/harassers: Cumulative 2000-2004. Retrieved Feb. 18, 2006, from Working to Halt Online Abuse Web site: http://www.haltabuse.org/resources/stats/2004stats/locationscum2004.gif.

Working to Halt Online Abuse (WHOA), (2003). Top six locations of harassers. Retrieved Feb. 18, 2006, from Working to Halt Online Abuse Web site: http://www.haltabuse.org/resources/stats/2003stats/harlocation2003.gif.

Working to Halt Online Abuse (WHOA), (n.d.). Cyber stalking laws: Pennsylvania. Retrieved Feb. 18, 2006, from Working to Halt Online Abuse Web site: http://www.haltabuse.org/resources/laws/pennsylvania.shtml.

Yanowitz, K. L. (2006). Influences of gender and experience on college student's stalking schemas. *Violence and Victims*, *21*(1), 91-101.