This is the published version (version of record) of:

Available from Deakin Research Online:
http://hdl.handle.net/10536/DRO/DU:30024054

Reproduced with kind permission of the copyright owner.

Copyright : 2009, Australian Council for Computers in Education
Cyberbullying research: The current state

ABSTRACT
This paper contributes to the understanding of cyberbullying by summarising the key themes in an up-to-date review of the academic research literature. The misuse of, and abuse in, online environments is ever-increasing and becoming a growing concern for educators, families and authorities around the world. It needs investigation to be understood and prevented to ensure safe and beneficial experiences for children and adolescents through networked and mobile communications. The various types of malice are described as is the frequency of their occurrences and the most prevalent tools for inflicting harm. Given this fast emerging global problem and the scarcity of empirical studies, there is a strong and urgent need for further research in.

INTRODUCTION
Electronic devices such as computers, mobile phones, digital camera and their ability to link to cyberspace hold great potential for both use and misuse. Cyber abuse is a result of fast developing and easily accessible technology. It is also referred to as cyber violence (Herring, 2002) and cyber bullying (Willard, 2004; Kowalski, Limber and Agatston, 2005) with a sub-category identified as sexual harassment by Barack (2005).

This paper documents existing research on the issue to gain a comprehensive picture of the current situation. It aims to raise awareness of the problem, stimulate debate, promote prevention and encourage further research. The paper starts with the various forms and characteristics of cyber violence, progresses into incident rates, dominant usage patterns and then the effects on the victims.

Background
Australian households and schools are digital technology rich and become increasingly more connected with mobile and online communication tools. The ABS (2008) reported that at the end of June 2008, there were 7.23 million active Internet subscribers in Australia. The majority of 6.21 million were households, business and government comprised 1.02 million subscriptions. More than 11.5 million Australians were online every month during the period of 2007-08 making them very active users. Fifty-five per cent of Australians were using the Internet more than eight times a week and were therefore identified as ‘heavy’ users. Also as of 30 June 2008; there were 22.12 million mobile phone services in operation (ABS, 2008). Given a population count of 21.37 million at that time, this equates to roughly one mobile phone in operation for every Australian. In terms of computers, ninety-eight percent of Australian families owned one while nine in ten families had Internet connection. (ACMA, 2007). The 2007-08 Communications Report by ACMA (Australian Communications and Media Authority) found that young people spent half of their discretionary time with electronic media and communications activities. This covered watching television, using the Internet, playing video or computer games, listening to music, watching DVDs and using a mobile phone. Children (aged eight to 11) spent an average of 30 minutes online per day, which increased to one hour and 32 minutes per day for teenagers (aged 12 to 14) and two hours and 24 minutes for adolescents (aged 15 to 17). Online communication activities for young people (eight to 17 years) comprised on average 49 minutes per day. Most popular were messaging and chatting (18 minutes), online gaming (15 minutes), using social websites (11 minutes) and emailing (five minutes). Authoring of web content gained significant responses, with 39 per cent of youngsters in this age group holding a personal profile on a social networking site (e.g. MySpace, Facebook). Thirteen percent had their own website and seven percent had created their own blog. More than half of the young people’s cohort (54 per cent) had their own mobile phone but more girls (63 per cent) than boys (46 per cent). Per day, girls also spent more time (an average 23 minutes) than boys (13 minutes) on their mobile phone (ACMA, 2008). The overall time spent online was the same for both genders although boys and girls showed marked variations in their preferences for media. Girls were more likely to participate in social activities (e.g. using a mobile phone to text and talk, online messaging, visiting social networking sites and emailing) while more boys than girls played video or (online) computer games (ACMA, 2008).

Given the large amount of time that young people spend on using electronic media and communications, there is an increased potential for misuse that may harm them in many ways.

Definitions and categories
The misuse and abuse of mobile and networked technologies through behaviours such as threatening others, indulging in hate-speech, online stalking, sexual remarks, vulgar language, bullying and harassing is known by many names. The ranges of terms include cyber abuse, cyber misuse, cyber harassment, cyber violence, cyberbullying (also spelled cyber-bullying), online bullying and online harm, with the spotlight being on the ‘dark side’ of the Internet. A more affirmative slant
has generated manifestations such as Internet safety, online safety, digital safety and cyber safety with the emphasis on pro-active strategies for self-protection. The often interchangeable use of the terminology without clear definitions of the associated behaviour causes misunderstandings and thus hinders the dialogue. Mapping the terms and characteristics (see Figure 1 below) endeavours to overcome this confusion.

The map is a compilation of the work by Herring (2002), Willard (2004), Belsey (2005), Barak (2005) and Kowalski, Limber and Agatston (2005). The central issue the intentional hurting of another person through mobile or networked communications.

**Figure 1: Overview of cyber abuse terms and characteristics**

Susan Herring (2002) used cyber violence to label all harmful online activities while distinguishing four separate categories: harassment, degradation, cyber stalking and a hybrid form labelled online contact/offline harm. This crossover from online to real life situations consists of initial contact via the Internet to gain a person’s trust, which moves to face-to-face interactions. At the onset, the criminal intent is to either take sexual or financial advantage of the victim or cause physical damage. Cyber stalking – similar to stalking in real life – aims to monitor another person’s activities and invade their privacy through unwanted contact. Degradation is words or actions that annoy, alarm or abuse others. Examples are threats, defamation of character, vulgar language and personal attacks. Denigration is the use of a “put down” of individuals or groups (Herring, 2002).

Nancy Willard (2004) devised seven categories of cyber bullying. While some labels are identical to Herring’s (2002), the characteristics of the behaviour varied; for example online harassment is described as the repeated sending of offensive message to a person while she sees cyber stalking as the intimidating of a person through threats and denigration as the false or cruel information about a person. Other categories are masquerade (defined as pretending to be a person and sending inappropriate material in their name so they will suffer the backlash of complaints, broken relationships and possible litigation), outing (identified as the circulating of sensitive or embarrassing material such as private emails or images) and exclusion (intentionally leaving somebody out from an online group). Willard (2004) describes flaming as the sending of angry or rude message about a person; which differs from its understanding in discussion boards or Internet Relay Chat (IRC), where it is also used to refer to long and heated discussions.


**Traditional bullying and cyber bullying**

Traditional bullying in schools may be physical (hitting, spitting, kicking) or verbal (teasing, ridicule, sarcasm, deception) in nature. Targets of bullying in schools are often peers who are considered strange or different by their peers. Bullying involves at least two people (perpetrator and victim) and possibly an audience of bystanders (Campbell, 2005).

Bullying amongst young people was been seen as a normal part of growing up. In the past, aggressive, intentional and repeated behaviour of an individual or a group against a target was not seen as a serious problem in schools (Campbell, 2005; Limber and Small, 2003). This wide spread acceptance of peer abuse changed in the 1990’s, when a wave of school shootings swept across the United States. In that decade, 14 separate incidents took place resulting in 49 deaths, with the Columbine High School massacre (on 20 April 1999) being the most violent (BBC News, 2007; Rosenberg, 2009). Investigation uncovered that all shooters had been bullied repeatedly by their peers prior to the assault and that school administrators failed to intervene (Dedman, 2000). Subsequently, anti-bullying programs and zero-tolerance policies were introduced into schools to eliminate bullying. A total ban of bullying in schools and the parallel arrival of cheap, fast and easily accessible networked communication technologies may have contributed to a shift from these traditional behaviour patterns into online contexts. This is
congruent with Li's view (2004) that cyberbullying is simply bullying in a new territory. Ybarra and Mitchell (2004) deduced from their findings that the victims of real-life bullying turned into online perpetrators. This role-reversal seems intuitively right as it allows face-to-face bullied victims revenge through cyber bullying while hiding behind their computer screens. Protected by anonymity, the previously powerless victim in traditional bullying situations turns to a powerful tormentor online, thus propagating the cruelty. However, the correlation between face-to-face bulling and cyberbullying with subsequent perpetuation of viciousness needs further investigation.

Both traditional bullying and cyberbullying have the same basic motivation: retaliation (revenge for having been violated) and the perpetrator's desire for power and control (Shariff, 2008). Although cyberbullying might be seen as 'safer' due to absence of physical violence, suicides of young people as a result of cyberbullying are now increasingly reported in the media (Halligan, 2005; ABC News, 2007). These examples show cyber bullying is not to be taken lightly.

Characteristics of cyberbullying

Cyberbullying has several unique features, which makes it hard to investigate and eradicate. Obscurity is one of them, as pseudonyms and well disguised IP addresses enable anonymity for the offender. "Disturbingly, most cyber-bullying is anonymous because perpetrators are shielded by screen names." (Shariff & Gouin, 2005:3). This makes it extremely difficult to detect and then stop these offenders. In a study of 177 Canadian middle school students Li (2005) uncovered that 41% of victims did not know the identity of their tormentor. This is not to say that the online abuser is a stranger, as "...class-mates who may not engage in the bullying at school, can hide behind technology to inflict more serious abuse." (Shariff & Gouin, 2005:4). In fact, a UK survey of 770 pre-teen and teens found that almost three-quarter (73%) of the cyber victims knew the bully; only one-quarter (26%) declared the perpetrator was a stranger (National Children's Home, 2005). The figures expose the significance of an established relationship between cyber bully and victim. It leads to the conclusion that the motive for the abuse is grounded in the history of their interaction. This might also account for the fact that girls were significantly more likely victims of cyber bullying than boys (Shariff & Gouin, 2005; Smith, Mahdavi, Carvalho & Tippett, 2006 and Li, 2005). A study of 1500 youngsters reported that girls are targeted twice as much as boys (Mitchell & Wolack, 2000).

The higher incidents of female cyber bully victims might be attributed to their heavier involvement in chat-based environments (e.g. using a mobile phone to text and talk, online messaging, visiting social networking sites and emailing) and thus greater exposure to possible violations, whereas boys played more video or (online) computer games (ACMA, 2008).

 Silence from cyberbullying victims, specifically their lack of reporting their online experience to their parents or another adult, was the most likely behaviour of targets (58%) according to a British survey conducted in 2005 (National Children's Home). Replies indicated that 31% did not report it because they did not think that it was a problem, 12% thought that there was no one they wanted to tell, 11% did not report it because they thought it would not stop the bullying or threats and 10% simple did not know what to do to get help (National Children's Home, 2005). Little wonder that "...incidents of online bullying are like roaches: for everyone that's reported, many more go unrecorded" (Chu, 2005:42). Reporting of being cyber bullied is one side, reporting to being a cyber bully is the other. Surprisingly, 8% of 10-12 year olds acknowledged their online harassment, while 27% of 13-14 year olds confessed to cyber bullying (Ybarra & Mitchell, 2004). The low self-reporting figures compared to the high incidents conveyed by the victims suggest that offending children either did not know that they were online abusers, did not admit to abusing online to avoid repercussion or that a small number of offenders inflicted a lot of the harm. While a correlation between admitting to online bullying and age existed, there were no gender differences. "Males and females were equally likely to report harassing another person online in the past year." (Ybarra & Mitchell, 2004:12). This evident lack of reporting and recording gives explanation to why hardly any teachers, principals and school administrators are aware that students are being cyber bullied (Beran & Li, 2004). Others actively ignored cyber bullying to avoid drawing attention to their institution, to side step dealing with it and subsequent entanglement in an unpleasant episode. This failure by staff to address and stop cyber bullying allows the behaviour not only to continue but increase (Giroux, 2003). The lack of intervention is tied to a lack of consequences for online abuser; unlike traditional bullying which is often followed up with some form of disciplinary action (i.e. detention, suspension from school).

Any one of these factors thwarts follow-up, allowing the perpetrators to remain anonymous and continue their malicious activities without reprimand. Their damage is exasperated by the permanency of their abuse and an unlimited audience as altered photographs of their victims, defamatory comments or untrue messages can be downloaded, saved and forwarded to others indefinitely, even if the offending content had been removed from the original site.

Historical review of empirical data on cyberbullying

Cyberbullying – due to the recent existence of the Internet - is still a very new phenomenon. Most scholarly writings have been from the legal perspective (i.e. policing and regulating of cyber crimes, the prosecution of cyber criminals), the technological area (i.e. prevention and detection software) and the discipline of psychology (i.e. counseling of victims). From an educational perspective, writings on cyber bullying span practical guidance, individual or multiple case studies, anecdotal observations, opinion and/ or position papers and engagement with current and future policy direction. Research findings have emerged from English-speaking countries while in other parts of the world (i.e. Asia) studies are just beginning to get underway. Hence, the body of empirical studies on cyberbullying in educational contexts is only growing slowly. The overview below (see table 1) has
be created to capture the body of work that used a quantitative approach. These surveys are listed in chronological order, by sample size, age group surveyed as well as by country and source.

The majority of existing empirical studies centre their attention on peer-to-peer cyberbullying of middle schoolers or adolescents. The focus is on the most frequent and most typical online incidents, the tools of cyber bullies, the extent of the abuse, the level of anonymity and profile of the perpetrator as well as the degree of reporting and attention from the authorities in response to episodes. The risk in online environments for children and adolescents had been recognised as early as 1999 according to Beckerman and Nocero (2003). The US Department of Justice, Washington D.C. commissioned the National Center for Missing and Exploited Children (NCMEC) to conduct the first scientific study of unwanted sexual material, solicitation and harassment online. As a result, the research team of Finkelhor, Mitchell and Wolak (2000) published Online victimization: A Report on the Nations’ Youth with the findings intended to make the Internet safer through education and prevention programs. This mindset underpinned the empirical studies for the last decade, while the main cyberbullying related finding across that period was an increase in frequency and escalation of severity.

Cyberbullying between students, their peers and teachers

As indicated earlier in the paper, the research on cyberbullying so far has concentrated on peer-to-peer hostility as this is the most common form and was the traditional behaviour pattern in schools. Shariff (2008:194) adds anti-authority cyber insubordination or anti-authority cyber-expression as another variant. These anti-authority online expressions by students engaged in defamatory speech or harmful acts against authority are either general in nature (for example the school as a target) or specifically targeted towards a particular person (a teacher or principal). Frequently they involve comments about appearance, hygiene, sexual orientation and teaching style, which can have significant impact on teachers’ self-confidence and trust in how they are perceived by the public (Shariff, 2008:151). She reports numerous events were students demeaned educators or other school staff by joking about them, insulting them, modifying photos or encouraging other students to get involved.

Shariff (2008:194) advises that both peer-to-peer bullying and anti-authority cyber-expression is walking the fine line between the right of free expression and breach of criminal laws. She notes that many aspects of cyber-bullying are clearly criminal in nature (such as threats of violence, criminal coercion, terrorist threats, stalking, hate crimes, child pornography and sexual exploitation). If brought before the court, they would most likely be subject to prosecution. For example, child pornography and sexual exploitation, which might be adolescents taking an explicit photo of themselves or others and sending it to their friends or a potential love interest. While this may seem like harmless flirting to some, any image depicting a minor in sexual activity or indecent manner is considered child pornography. Anyone who passes on or receives those images is liable to face criminal charges. This was the case with 32 Victorian teenagers who were charged with child pornography offences during 2007 alone (Battersby, 2008).

Blurred boundaries

Cyberbullying creates a tension between the right of free speech by the offender and the right for safety or protection from defamation by the victim. Perpetrators might argue that they were engaged in private conversations with their friends when their slanderous and libellous comments were made. This blurring of boundaries between free expression and safety is further blurred with the issue of privacy and supervision as students object to adults’ control of their online communication. In terms of monitoring and preventing young people from online bullying, there is also disagreement between educationalists and parents about who should take responsibility for addressing it. The fluidity between private and public, physical and virtual spaces is even more complicated because of the spillover effect. For example, cyberbullying at night on a home computer can easily continue the next day at school (i.e. in the computer lab, on a laptop, mobile phone) or morph into face-to-face bullying.

In terms of the physical location for cyberbullying, research findings are conflicting and thus inconclusive. For example, the British National Children’s Home (2005) found that half of all cyberbullying (48%) occurred at school or college and the other half (44%) outside. The low rate of incidents on weekends (17%) and during school holidays (6%) might be attributed to travel and leisure activities, with schedules reducing opportunities to use the Internet. Inappropriate use at school or college might be a combination of inadequate supervision combined with easy access. Contrary, the British scholars Smith, Mahdavi, Carvalho and Tippett (2006) found that cyberbullying happens mostly outside school. They sampled (three year) younger adolescents with the upper age limit of their participants being 16 years. These young people would not have driving licenses and thus mobility to engage in a range of activities during their spare time but may use mobile and online communication tools instead to connect to their peers.

Lower rates of cyber bullying in the schools captured by their research might be due to close supervision by teachers. In the home environment, parents’ lack of technical skills and awareness might result in minimal scrutiny of the child’s online activities. Another reason might be the electronic filtering devices installed in school networks and desktops, whereas protective software might be absent or outdated on home computers. In addition, it could be speculated that some schools have “acceptable use” policies (stipulating the guidelines for use and the repercussion for misuse of the internet), which are signed by students and may act as a deterrent.
Impact of cyberbullying

Anecdotal evidence suggests that the effect of cyber bullying is more damaging than traditional bullying and has longer lasting effects. Shariff (2004:9) believes that cyber bullying "creates a hostile and negative school environment..." and that this substantially disrupts learning, causing damage to the emotional wellbeing of young people in schools. Due to the parallels between bullying and cyberbullying in terms of motivation and pattern of behaviour, Shariff (2004) surmise that the negative effects are also similar.

In face-to-face bullying, both victims and bullies experience more psychosomatic problems (i.e. depression, anxiety, low self-esteem) than those not involved in bullying (Juvonen and Graham, 2001; Rigby 2001). In traditional bullying, bystanders also suffer although they only witness an incident but remain uninvolved. Usually, fear is holding them back, particularly if they are worried that intervention might draw attention and turn them into next victim. As a result of observing bullying incidents, loss of self-respect and self-confidence is often experienced (Campbell 2005). By and large, the behaviour patterns between traditional and cyber bullying seemed to be comparable. In attempting to detect and prevent harm, Smith, Mahdavi, Carvalho and Tippet (2006) advocate research to probe into the nature of cyberbullies to develop a perpetrator profile for their identification. Exploring attitudes and reasons for cyberbullying might help in developing effective prevention and counteraction strategies.

CONCLUSION

This review paper focused on cyberbullying, highlighting the lack of empirical studies and limited knowledge of the issue to provide effective counter strategies. The few qualitative studies providing evidence on the phenomenon focus on the extent and nature of the problem and document the rapid increase of cyberbullying over the last few years. For example, the same research team found an increase in cyberbullying from 28 percent to 48 percent within 5 years, specifically from the time of their first study in 2000 to their second study in 2005 (Finkelhor, Mitchell & Wolak, 2000; Wolak, Mitchell & Finkelhor, 2006). This rise took place despite the use of filtering and blocking software on computers and notwithstanding numerous Internet safety websites, initiatives and campaigns from non-profit organizations, commercial providers and governments.

The abusers' "invisibility" while hiding behind a computer screen, the relationship between the victim and the perpetrator, the lack of online abuse incidents reported to adults and the subsequent lack of follow-up are further concerns.

Researchers have yet to examine the initial motivation for, the dynamics with online bullying incidents and subsequently effective prevention of cyberbullying. This understanding could be used to develop more effective strategies for combating cyberbullying than those that are currently in place. In finding counter-strategies, the parallels between traditional face-to-face bullying behaviour and cyberbullying were examined but expecting the same issues and problem solving approaches may be over simplistic. While there might be a correlation (Li, 2004; Yabarra and Mitchell, 2004; Shariff, 2008) school staff parents and young people themselves can not be given any evidence based principles in dealing with cyberbullying because of the lack of empirical research data. While anecdotal cases shed some light onto the reasons and behaviour of a single offender, those individual reports do not provide a comprehensive picture of the rationale for choosing a particular kind of abuse or technology over the other. Once again, scientific research will shed light on the motivations for and prevention of cyberbullying. This research evidence is needed to design cyber safety programs for students, teachers, parents and the wider community. Cyber-safety instruction courses - based on research evidence – could be incorporated into training courses for professionals working with young people (i.e. teachers, youth workers, psychologist, counsellors). This awareness and instruction could be linked to mandatory reporting, which already exist in relation to physical maltreatment and sexual exploitation, in order to include online abuse. An obligation by law to report specific forms of cyber abuse would send a clear message to abusers that their acts have been recorded and will be followed up and penalized. Prior to that, acceptable use policies and codes of practice for appropriate online behaviour would have to be compulsory introduced to cover safety, privacy and responsible use. In addition, help for victims of online abuse needs to be available. This requires substantial funds, which need to be dedicated not only to investigate the under researched area of cyber violence but also to provide methodical research to determine future policy. The forming of a global working party and a global register for repeated and extreme online perpetrators to monitor or restrict their future activities might be needed since cyber abuse is not limited by national borders.

In closing, current initiatives have shown to be ineffective in reducing the rise of cyber violence. Therefore, heavy investment into cyber safety research and a systematic tackling of the problem through policy and practice on a national as well as worldwide scale is imperative.

BIOGRAPHY

DR. RIA HANEWALD is a Research Fellow at The University of Melbourne. An educator for more than two decades, Ria has taught at early childhood, primary, secondary and tertiary levels in Europe, Asia and Australia. She is interested in teacher professional development and conducting research on the use of Web 2.0 technologies for collaborative teaching and learning.
REFERENCES


