



GEELONG
CATS
FOUNDATION



Cyberbullying – Prevalence, Risk Protective Factors, and the Efficacy of Cyberbullying Interventions

A LITERATURE REVIEW

**Dr Bianca Klettke
Dominika Howard
Elizabeth Clancy**

Deakin University
School of Psychology
221 Burwood Highway
Burwood VIC 3125
Bianca.klettke@deakin.edu.au

Contents

Executive Summary	3
About cyberbullying	3
Risk factors	4
Protective factors.....	5
Theoretical basis for anti-cyberbullying programs.....	5
Cyberbullying prevention and intervention programs	6
Cyberbullying program delivery and evaluation	7
Conclusions	8
Literature Review	9
What is cyberbullying?	9
Prevalence rates of cyberbullying	12
Consequences of cyberbullying.....	13
Risk factors.....	13
Cyberbullying perpetration	13
Cyberbullying victimisation	15
Cyberbullying bystanding	17
Protective factors against cyberbullying.....	18
Cyberbullying perpetration	18
Cyberbullying victimisation	20
Cyberbullying bystanding	21
Theoretical basis for anti-cyberbullying programs	21
Cyberbullying prevention and intervention programs	22
Cyberbullying prevention/intervention programs and associated challenges	25
Gaps in the literature and recommendations for future research	27
Study limitations	28
Conclusions	28
References	30

Executive Summary

This review was commissioned to inform a review and evaluation of the Geelong Cats' school-based anti-cyberbullying program, Cybercats, to ensure it is evidence-based and encompasses best-practice principles. The review aimed to:

- i. identify risk and protective factors associated with adolescent cyberbullying perpetration, as well as victimisation and bystander behaviours.
- ii. assess effectiveness of cyberbullying prevention and intervention programs
- iii. provide recommendations for new program development and implementation.

The review involved a scan of available literature via academic databases and Google Scholar, with a focus on systematic reviews. However, grey literature, such as policy resources, was not incorporated in this search, and much of the existent research and evaluation was descriptive in nature, hence statistical approaches were not applied.

About cyberbullying

Cyberbullying can be considered an aggressive behaviour, whereby harm is intentionally inflicted by one or more people through electronic means. Many definitions also emphasise repeated behaviours, power differentials and deriving gratification from mistreating others who find it hard to defend themselves. However, there is contention over some of these aspects, including intentionality, power imbalances and repetition in these definitions.

Cyberbullying behaviours are prevalent in adolescence, with 10-40% of adolescents having experienced cyberbullying, while 19% report having both experienced and perpetrated cyberbullying, and 2% report solely having cyberbullied others. Cyber bystanders overwhelmingly outnumber cyberbullies and victims, with one study finding 88% of respondents had witnessed cyberbullying instances, and 91% of that group remained passive observers. Bystanders have a critical role, given the potential to either support a victim, support the bully, or be an inactive observer. As cyberbullying behaviours are becoming increasingly common, the crossover from traditional bullying is also increasing, with victimisation rates of 21% in 2012.

In addition to the potential legal ramifications, this review outlines the various negative emotional, psychological, social and physical consequences of cyberbullying behaviours for victims and perpetrators. As such, greater investigation is warranted to determine key risk

and protective factors for all cyberbullying activities, and to evaluate existing programs against this information.

Risk factors

This review identifies risk factors associated with all types of cyberbullying behaviours, across individual, interpersonal/social and community level factors, as indicated below.

For **perpetration**, individual risk factors include having been victimised oneself, age (peaking in early-mid secondary school years), time spent online, views accepting or normalising aggression, as well as psychological factors, e.g., moral disengagement, risky online behaviours, lower self-control, thrill-seeking behaviours and impulsivity. Social and community risk factors relate to school engagement and poorer relationships with parents.

Risk factors for **victimisation** include (at the individual level), being a victim and a perpetrator of traditional bullying, anger, risky online behaviour, frequency of internet use, moral disengagement, and hyperactivity. Other factors such as lack of self-control, social anxiety, aggressive thoughts and antisocial behaviour, low social intelligence and empathy have also been associated with cyberbullying victimisation. Age is again a risk factor, with some research also indicating that females might be at greater risk. Interpersonally, poorer parent-child relationships and a lack of parental supervision during online activity are also associated with increased risks of online victimisation. Community factors include minority identification, e.g. racial groups, persons with chronic health conditions as well as persons with a history of sexual abuse, all of whom are more likely to be cyberbullied than their peers.

Cyberbully **bystanding** risk factors suggest that intervention in cyberbullying is less likely when other bystanders are present, either passively or joining the bully, when a call for help is sent to more than one recipient, when acts are insidious, and more ambiguous, and where victims' response are not readily available. Intervention is also less common when the perceived risk is high, for example when the perpetrator is popular, the bystander feels they would not receive support from others, are afraid of consequences for taking action or damaging a relationship with the bully; have low self-efficacy by believing they do not have the necessary skills or ability to intervene; or have lower levels of affective empathy.

Protective factors

Family-based protective factors which reduce risks of **cyberbullying perpetration** include adequate parental supervision and interest in children's lives, secure family environments and positive parent-child relationships marked by mutual trust and communication.

Community-based protective factors include school connectedness, a sense of safety and school-based programs, policies and procedures, as well as positive relationships between students, school staff and parents, which is consistent with a socio-ecological approach that addresses individual, familial, school and community levels.

Individual protective factors against **cyberbullying victimisation** include higher self-esteem and empathy, emotional intelligence and emotion regulation, and confidence in the ability to defend oneself. This is also supported by access to professional counselling to address factors such as anxiety or social withdrawal.

Social protective factors include peer, family and school supports, which buffer negative effects on mental health, substance use and reduce subjective health complaints.

Community level protective factors include perceived school safety, positive school climate, greater school satisfaction and residing in safer neighbourhoods.

Individual factors found to increase the likelihood of **bystander intervention** include greater self-efficacy in the ability to assist and positive outcome expectancies, empathy towards the victimised person and acceptance of diversity, e.g. cultural, sexuality or physical differences.

Social factors which increase bystander intervention include modelling behaviours that disagree with and reject online aggression, witnessing disapproving reactions towards cyber aggression exhibited by others, receiving direct requests for help, being a friend of a victim and when other bystanders are friends of the victim.

Theoretical basis for anti-cyberbullying programs

Most anti-cyberbullying programs operate within a bio-psycho-social framework which emphasises interactions between an individual and their environment across inter-related individual, family, school and community levels. Events experienced in one system may influence functioning in another, and hence change is best achieved by addressing factors at multiple levels.

Cyberbullying prevention and intervention programs

Given the significant social concerns associated with cyberbullying, various countries have introduced legislation with regards to this behaviour, which, in turn, has been found to reduce reports of cyberbullying. Such legislation aims to provide clarity pertaining to:

- descriptions of bullying behaviours
- scope of application and in what circumstances organisations can act
- obligations for local authorities, including schools, to develop and implement relevant policies within a set timeframe

This review identified that the majority of programs actively seeking to tackle bullying and cyberbullying are school-based, and adopt one of two approaches:

- Universal interventions aim to change overall school climate and decrease peer aggression, and operate across multiple levels, including individual students, classrooms, schools, and parents
- Focused interventions are designed for specific subgroups such as victims, bullies, and bystanders, and operate on a single level.

Universal interventions tended to be more effective in improving school climate and student well-being, and reducing negative consequences of victimisation, but long-term effects have often dissipated by follow-up. Overall, evaluations of cyberbullying or online aggression prevention and intervention programs have had mixed findings. Programs vary with respect to their aims, modes of delivery, duration and intensity, involvement of parents, teachers and wider community, and variability in the rigour of evaluation was an issue in some cases.

However, a number of specific program components have been found to decrease cyberbullying behaviours. These include

- parent education
- communication and social skills training in both online and offline settings
- empathy training
- coping skills and strategies to cope with online aggression, and
- digital citizenship.

Changing attitudes towards cyberbullying and improving self-efficacy appears less effective, and there was no consistent relationship between program duration and outcomes.

Cyberbullying program delivery and evaluation

As noted above, evaluations of existing programs are limited and variable in quality. For any future program, robust evaluation is critical to engender confidence among decision-makers and program facilitators that a given approach is grounded in solid and evidence-based research, and likely to deliver successful outcomes. Robust evaluation should include:

- study designs (experimental or quasi-experimental), that allow for causal inference
- data collection at baseline, post program and follow-up at 6 and 24 months
- multiple data sources, such as students, teachers, and parents.

A focus on program fidelity is also important, with cyberbullying programs benefiting from standardised training and delivery approaches, for example:

- a published manual and/or website, which details the program's underlying theoretical basis, assumptions and definitions, delivery plans, and cost
- facilitator and staff training and support
- assessment tools
- program monitoring and maintenance strategies

These aspects should be balanced with sufficient flexibility to meet local schools' objectives. Ideally, evaluations would also be supported by common definitions and an agreed, valid and reliable measurement instrument, which would allow for direct program comparisons.

Although uniform definitions and measurement tool may be a longer-term challenge, positive moves include:

- application of multiple-item psychometric tools as opposed to single-item measures
- providing a definition of cyberbullying behaviours and the word "bully"
- measuring traditional bullying (victimisation and perpetration) behaviours as well as online forms.

In addition to the above, there is a paucity of delivery and evaluation of programs in non-school settings or targeting specific population or younger groups. This would benefit from the following:

- Evaluation of programs delivered outside school settings and/or by community members.

- Focus on specific target groups at increased risk of cyberbullying, e.g. youth with disabilities, or minority identification, and program outcomes for these cohorts.
- Development and evaluation of age-appropriate cyberbullying prevention programs for younger students, to reduce rates of future victimisation and perpetration.

Conclusions

Cyberbullying is a prevalent form of online peer aggression, linked to various psychological, behavioural and social problems. Variables associated with risk factors for cyberbullying perpetration, victimisation, and cyber by-standing among adolescents are numerous, and require attention on multiple levels. This review has indicated that legislative approaches can be effective in decreasing cyberbullying. Prevention and intervention programs that target whole-school environment, involve parents, teachers, and students, thereby engaging all levels of the environment in which teens develop, also tend to decrease cyberbullying perpetration, victimisation and bystanding.

The current review also describes challenges associated with evaluating cyberbullying prevention and intervention programs, with recommendations for future research. Gaps in current knowledge are identified, including a scarcity of cyberbullying community-based programs delivered by non-school staff and knowledge regarding their effectiveness. Future research should consider exploration of cyberbullying prevention and intervention programs within local communities as they may also prove successful in regards to changing the culture around cyberbullying, thereby decreasing instances of peer online aggression.

Literature Review

What is cyberbullying?

Cyberbullying has been defined as a form of aggressive behaviour, whereby harm is intentionally inflicted upon individual(s) by a single person or a group of people through electronic means, such as computers or mobile phones. Moreover, the acts of online aggression are carried out repeatedly by persons who perceive themselves to be in the position of power and derive personal gratification from mistreating the victim(s) who find it hard to defend themselves (Patchin & Hinduja, 2006; Smith et al., 2008).

Further, Langos (2012) has extended this definition to identify two types of cyberbullying behaviours: in the first one, termed direct cyberbullying, cyberbullies channel their aggression directly towards their targets by, example being, sending mean messages to the victims' phones or email accounts. In the second type, termed indirect cyberbullying, harmful material is posted in a public arena, to which the victims may or may not have access to or have the awareness of. While direct cyberbullying requires the involvement of at least two parties, the cyberbully and the cybervictim, indirect cyberbullying often occurs in the presence of bystanders.

While the definition of cyberbullying has been derived from the literature on traditional bullying (Nocentini, Calmaestra, Schultze-Krumbholz, Scheithauer, Ortega, & Ersilia Menesini, 2010; Olweus, 1993), researchers have challenged the applicability of intentionality and repetition to the concept of cyberbullying, and have also reinterpreted the notion of power imbalance in the context of online aggression. For example, Langos (2012) has argued that the intention to harm the victim may not always be obvious, especially in cases of indirect cyberbullying whereby the aggression is not enacted directly towards the targeted person. Examples of indirect cyberbullying are situations in which harmful material is posted in a private or public forum to which the victim may or may not have awareness of or even access to. Another example of indirect cyberbullying may be the distribution of sexts, which are defined as sexually explicit messages, images, or photos usually sent via mobile phones (Klettke, Hallford, & Mellor, 2014). In these cases, sexts, which were intended for a

specific recipient, are forwarded to third parties without the knowledge or permission of the original sender. It has been proposed that the intention to harm in such circumstances, although obscured, could be established through the hypothetical reasonable person approach, whereby the acts of the perpetrator are judged by a person adopting the position of a victim (Langos, 2012).

Repetition of the cyberbullying acts as a necessary aspect of the definition has also been questioned. As Langos (2012) rightly observes, once any material is posted in cyberspace in the public arena, it remains there indefinitely as it can be saved, archived, copied, and reposted ad infinitum by other users. Moreover, the harmful content such as an embarrassing photograph or video, although created and uploaded onto the Internet once, may constitute a source of repeated degradation and humiliation of the victim (Dooley, Pryzalski, & Cross, 2009).

Further, in traditional bullying, the source of the power imbalance may stem from the fact that the perpetrator is physically or psychologically stronger, older, or more socially popular than the victims (Dooley et al., 2009; Juvonen & Graham, 2014), implying it is harder for the targeted persons to defend themselves. In a cyberbullying scenario, this power inequality may manifest itself differently. Specifically, the perpetrator(s) may remain anonymous, exhibit greater technical savviness through concealing their phone number, extend harm by gathering a large audience of online bystanders, or carry out the acts of aggression irrespective of time and whereabouts of their victim (Dooley et al., 2009; Kowalski, Giumetti, Schroeder, & Lattanner, 2014; Langos, 2012; Patchin & Hinduja, 2006, Snakenborg, Van Acker, & Gable, 2011). However, similar to traditional bullying, the aforementioned factors exclusive to online aggression may instil a sense of helplessness and being dominated in victimised persons. This may especially be the case as many victims may not know who their perpetrators are, nor have the right skills or resources to stop the abuse or defend themselves.

As can be noted from the above discussion, identifying cyberbullying behaviours may sometimes prove challenging due to the intricacies associated with the definition of this behaviour. It may also be further complicated by the rapid advances in modern-day technology, which, by virtue of its exponential growth and sophistication, constantly creates new avenues for the perpetrators to abuse their victims (Nocentini et al., 2010). Nonetheless,

research to date has identified a number of behaviours carried out by means of the Internet and electronic devices that constitute common examples of cyberbullying (Canton et al. 2015; Chisholm, 2014; Notar, Padgett, & Roden, 2013; Willard, 2007). These encompass, and are not limited to, the following:

- *flaming* – posting insults or initiating verbal fights by using angry, mean, and vulgar language. Messages can be supplemented with graphics and images;
- *shock trolling* – publicising mean-spirited and nasty messages in a public arena with the aim to anger someone and provoke a response;
- *cyberstalking* – the act of aggressive, persistent, and threatening harassment aimed at instilling fear in a victim;
- *denigration/dissing* – spreading rumours or gossiping about a person with the intent to damage their reputation or relationships;
- *visual aggression* – posting and dissemination of harmful, visual material;
- *outing* – the act of sharing a person’s secrets or images online or through mobile phones;
- *slamming* – refers to a situation in which bystanders join the bully in teasing or harassing the targeted person;
- *masquerading/impersonation* – assuming someone’s identify or pretending to be someone else online in order to harass a targeted person, to ruin that person’s reputation or relationships, or to get the person in trouble;
- *catfishing* – tricking a person into an emotional, online relationship by assuming a fake identity and fabricating social relationships;
- *trickery* – coercing a person into sharing personal information, secrets, or images with an intent to post or share them online;
- *phishing* – attempting to obtain sensitive personal information, such as bank account or passwords, by pretending to be a trustworthy entity, a website you are familiar with, or a person you interact by phone, text messages or online;
- *rattling* – pertains to controlling someone’s computer or webcam without their permission or knowledge;
- *flooding* – an act of sending many lines of text to the victim to flood their screen with text;

- *sex dissemination* – purposeful and non-consensual distribution of sexts (sexually explicit messages, images, and videos);
- *exclusion* – deliberately excluding an individual from an online group or a gaming room; not playing by the rules, creating roving gangs and denying entryways in multiplayer online games;
- *griefing* –in online games, pertains to the acts of aggression and violence through hate-speech, killing a team member, virtual rape, or stealing virtual money or items.

As can be inferred from the extensive list above, human creativity has facilitated countless ways in which harm can be inflicted upon others online. Apart from the human factor, however, easy access to and the affordability of technology appears to parallel the growing trend of cyberbullying behaviours. A study by Schneider, O'Donnell, and Smith (2015) has revealed that cyberbullying victimisation increased from 15% in 2006 to 21% in 2012. Among the victims of traditional bullying, 35% indicated in 2006 that they also experienced cyberbullying, with this number increasing to 50% in 2012 (Schneider et al., 2015).

Prevalence rates of cyberbullying

According to the Australian Bureau of Statistics (2018), 86% of households in Australia were connected to the Internet in 2016-17, with teenagers aged between 15 and 17 being identified as the most frequent users (98%). Further, over a million of Australian teenagers between the ages of 14 and 17 have a mobile phone (91%) (Roy Morgan Research, 2016). Although not all users of technology engage in cyberbullying activities, the behaviour is nonetheless prevalent.

A recent cross-sectional study conducted among 2,338 youth in Australia between the ages of 12 and 18 has revealed that 27.7% of respondents reported being cyberbullied at least once in the past term. Moreover, 18.9% of respondents identified as both a victim and a perpetrator of cyberbullying, whilst 1.8% reported solely having cyberbullied others (Spears, Taddeo, Daly, Stretton, & Karklins, 2015). Findings from international research also indicate that online aggression constitutes a widespread social issue, with victimisation rates ranging from 10 to 40% (Kowalski et al. 2014).

With regards to the prevalence of cyber bystanders, previous research has shown that

cyber bystanders overwhelmingly outnumber cyberbullies and cybervictims. In a study conducted among US teens, Lenhart et al. (2011) found that 88% of respondents had witnessed instances of cyberbullying on social media, and 91% of that group remained passive observers. Bystanders play a critical role in cyberbullying behaviours because they have the capability to support the victim when cyberbullying takes place or constitute a part of the problem by either supporting the bully, or being inactive observers (Allison & Bussey, 2016; Notar et al. 2013).

Consequences of cyberbullying

Several negative psycho-social consequences have been identified as a result of cyberbullying. Persons who have experienced cyberbullying often report lower self-esteem and life satisfaction, increased stress, depression, anxiety, loneliness, sadness, anger and frustration, conduct and emotional problems, suicidal ideation, somatic symptoms, substance abuse, decreased social connectedness and reduced prosocial behaviours (Kowalski et al., 2014; Patchin & Hinduja, 2006; Spears et al. 2015; van Geel, Vedder, & Tanilon, 2014).

In the light of the devastating consequences that may arise from cyberbullying victimisation and the accessibility of digital technology affording the perpetration of online aggression, the current review sets out to review risk and preventative factors associated with cyberbullying participation, examines the efficacy of current prevention and intervention programs, and provides recommendation for the development and evaluation of future anti-cyberbullying programs.

Risk factors

The following section will summarise risk factors associated with cyberbullying perpetration, victimisation and passive bystanding.

Cyberbullying perpetration

Cyberbullying perpetration constitutes a complex behaviour that is associated with a number of cognitive, emotional, behavioural and social factors. A recent meta-analytic review revealed a number of factors that may predispose a person to become an online aggressor. For instance, being a victim of cyberbullying is strongly related to cyberbullying perpetration (Kowalski et al., 2014). In these situations, victims become bully-perpetrators as they use similar methods to their perpetrators to retaliate the aggression they experienced.

Being a traditional (face-to-face) bully is moderately associated with cyberbullying perpetration (Kowalski et al., 2014), which suggests that cyberspace constitutes another setting through which bullies can channel aggression against their targets.

Age has also been identified as an important factor in cyberbullying perpetration. According to a study examining cyberbullying across the lifespan (Barlett & Chamberlin, 2017), cyberbully perpetration increases from early teenagehood until early adulthood and then starts to decrease into older age, a trend which can be illustrated by means of inverted U-shape distribution. However, a meta-analytic review by Kowalski et al. (2014) has revealed that the strongest overlap between cyber and tradition bullying occurs when adolescents transition from middle to high school, suggesting that intervention programs should specifically target youth in grades from 7 to 10. With regards to gender, there is currently no consensus as to whether boys or girls are more likely to perpetrate online violence (Kowalski et al. 2014).

Use of technology and time spent on the Internet has been positively related to cyberbullying perpetration and victimisation. Specifically, among primary school-aged children, perpetration occurs through online games, whilst among teens, bullying takes place predominantly on social media (Kowalski et al.2014; 2018).

With regards to personal determinants, views accepting or normalising aggression, as well as psychological factors such as moral disengagement, online disinhibition, psychopathy, Machiavellism, narcissism, anger, risky online behaviours, lower self-control, thrill-seeking behaviours and impulsivity have been linked to perpetration of online aggression (Kowalski et al., 2014, 2018). Further, online aggression is associated with depression, anxiety, lower life satisfaction, lower self-esteem, lower cognitive and affective empathy, poorer academic achievement, higher levels of loneliness and delinquent behaviour including smoking, drug and alcohol use, school misconducts (Kowalski et al. 2014, 2018).

In addition to the intra-individual factors mentioned above, researchers have also focused on the relationship between cyberbullying perpetration and school, home and peer environment. Specifically, poorer school commitment, dislike of school, lack of teacher support, absence of clear rules pertaining to cyberbullying, weaker emotional bonds with the parents/caregivers, more frequent discipline by the parents, and poor parental supervision of children's online activities have been associated with cyberbullying perpetration. (Kowalski

et al., 2014, 2018). Children with poorer emotional bonds with their parents have been found to be more than twice as likely to engage in online harassment, and frequent punitive practices on the part of the parents such as yelling, have been linked to an increased likelihood of online aggression among adolescents (Ybarra & Mitchell, 2004). In contrast to frequent monitoring of youth's online activities, low parental supervision has been linked to a 54% increase in likelihood of harassing someone online (Ybarra & Mitchell, 2004). Negative influence of peers, lack of friends who would model positive values and behaviours, social rejection, and thus isolation have been established as significant predictors of cyberbullying perpetration (Kowalski et al. 2018).

While the aforementioned factors determine a greater likelihood for bullying behaviours, they do not answer the question as to why teenagers engage in online aggression in the first place. A literature review by Snakenborg et al. (2011) indicated that retaliation in response to traditional or cyberbullying is one of the reasons people engage in online aggression, followed by the desire to demonstrate technological savviness and power, for instance through the manipulation of images or the ability to remain anonymous. Also, the need to be affiliated with a peer group/social clique appears to entice some individuals to join the perpetrators or remain passive (for details, see Snakenborg et al. 2011).

Cyberbullying victimisation

Unsurprisingly, a lot of the risk factors identified for cyberbullying victimisation overlap with risk factors associated with cyberbullying perpetration, which can be explained by the fact that a large proportion of people who perpetrate cyberbullying are also victims of cyberbullying, and thus share common characteristics. Although any child or teenager can potentially fall victim to online cyberbullying, research has revealed a number of factors which may predispose a person to become a target. As cited by Notar et al. (2013), cyberbully victims are often bullied in a traditional way at school, are either bystanders or perpetrators of cyberbullying themselves, exhibit lower self-esteem, deem themselves to be less popular, are socially isolated, more likely to use the Internet, be active on social media, and exhibit risky online behaviours. A meta-analytic review by Kowalski et al. (2014) has found that the strongest predictors of cybervictimisation is being a victim and a perpetrator of traditional bullying, followed by anger, risky online behaviour, frequency of Internet use, moral disengagement, and hyperactivity. Other factors such as lack of self-control, social

anxiety, aggressive thoughts and antisocial behaviour, low social intelligence and empathy have also been associated with cyberbullying victimisation (Kowalski et al. 2018).

With regards to age and gender, a higher incidence of cyber victimisation has been noted during the time students transition from middle to high school (Notar et al. 2013), with middle school (grades 6 to 9) being identified as a period where cyberbullying victimisation becomes problematic and continues to escalate into high school (Kowalski, Limber, & Agatston, 2012). Some studies suggest that girls are more likely to be victims of cyberbullying than boys (Snell & Englander, 2010; Walrave & Heirman, 2011), though some researchers have found no gender differences in victimisation rates (Slonje & Smith, 2008). However, a positive relationship has emerged between being a victim of cyberbullying and depression among samples that contained a greater number of female respondents, indicating that the latter may be also experiencing poorer mental health outcomes in comparison to males (Kowalski et al., 2014).

Studies that investigated the immediate environment among high and middle school adolescents have shown that youth from single-parent households or families with a negative environment (e.g. marked by interpersonal conflicts), or that have poor relationship with their parents (poor attachment), or with a history of sexual abuse are more likely to be cyberbullied than their peers. Lack of parental supervision and/or strategies for the responsible use of technology along with the time spent online on the Internet for social and gaming purposes have been associated with an increased risk of online victimisation (Kowalski et al. 2018).

As some cyberbullying behaviours are underpinned by societal norms and thus prejudices, minority groups - sexual, ethnic- tend to be victimised more often (Hong & Espelage, 2012). An extensive review of the literature by Kowalski et al. (2018) has found that gay, lesbian, bisexual and transgender youth are at increased risk of cyber victimisation. Further, minority groups appear to fall victim to cyberbullying more often, however, Kowalski et al. warn that such conclusions cannot be drawn with confidence as a lot of studies do not provide sufficient information on the racial/ethnic density of the settings in which the studies were conducted. Further, adolescents dissatisfied with their appearance, and those with disabilities or chronic health conditions, for instance ADHD, have been found to be at an increased risk of being cyberbullied in comparison to peers with greater body

satisfaction, or who are healthy/typically developing (see Kowalski et al. 2018 for further details).

Cyberbullying bystanding

As noted previously, sometimes cyberbullying behaviours take place in front of an audience of online bystanders who may either choose to intervene by confronting the bully, reporting the abuse, assisting the victim, or remain inactive. The following section will examine factors that may contribute to the lack of response on the part of bystanders.

A literature review by Allison and Bussey (2016) has revealed that a person is less likely to intervene when other bystanders are present, when other bystanders are passive or join in the bully, when a call for help, in the form of an email, is sent to more than one recipient. However, the relationship between the number of bystanders and bystander inactivity is not linear, as online communities exceeding 250 members have been found to be more likely to respond to instances of online victimisation and to offer assistance as opposed to medium-sized groups (for more details, see Allison & Bussey, 2016). Further, instances in which cyberbullying acts are insidious, and thus more ambiguous, and in which victims' response are not readily available are less likely to elicit a response from the online onlookers (as cited in Allison & Bussey, 2016).

Drawing on the social cognitive theory by Albert Bandura (1990), the review by Allison and Bussey (2016) has also identified a number of cognitive processes, characteristic of moral disengagement, that predispose online bystanders to remain inactive. These include a) downplaying the responsibility to intervene by, for instance, deeming the incident as of not their concern; b) attributing the responsibility to take action to specific persons, such as popular/strong students or friends of the victims; c) attributing the blame for cyberbullying to the victims by perceiving them as provocateurs, unpopular, or outsiders; d) downplaying the effects of the abuse on the victim.

Further, bystanders are less likely to take action when the online perpetrator is popular, they feel they would not receive support from other online bystanders, are afraid of the consequences for taking action or damaging the relationship with the bully; have low self-

efficacy by believing they do not have the necessary skills or ability to intervene; or have lower levels of affective empathy (for detailed discussion, see Allison & Bussey, 2016).

The discussion above provides a wealth of information with regards to the factors that may put a person at risk of being a victim, perpetrator, and a bystander in the context of cyberbullying. The following section will, in turn, focus on the protective factors, as these are equally important in preventing the occurrences of online aggression.

Protective factors against cyberbullying

Cyberbullying perpetration

As cyberbullying often overlaps with traditional bullying, guidelines for the effective prevention of traditional bullying may prove informative in decreasing instances of online aggression. Research by Pearce, Cross, Monks, Waters, and Falconer (2011) has identified six domains of interventions against traditional bullying that proved efficacious in targeting traditional bullying, and hence may also prove useful in the prevention of cyberbullying perpetration. These domains encompass (a) school-level interventions through the adoption of programs that are evidence-based, and having sufficient resources such as funding, materials, adequate staff training, and longer time frames for trialling anti-bullying programs. Further, (b) fostering students' connectedness to their school by creating positive and safe school environment, promoting open discussions about peer aggressions, having students involved in developing classroom rules against bullying, and encouraging peer interventions proved successful in reducing bullying incidents. The adoption of formal anti-bullying policies (c) with clear procedures for action have been found to support safer school climate environments and also sends a strong message against anti-social behaviours, which are also typically associated with lower incidences of bullying behaviours. Moreover, involvement of parents and school staff through (d) the provision of parental and teacher education pertaining to bullying, (e) enhancement of positive relationships between students and school staff, and (f) the involvement of wider community, families and local organisations have also been found crucial in reducing bullying.

As can be noted from the above points, safe school environments and a supportive school climate are critical factors in the prevention of cyberbullying. For instance, Sourander

et al. (2010) indicated that not feeling safe at school constitutes a risk factor not only for cyberbullying victimisation, but also for cyberbullying perpetration, and being a cyber bully-victim. The authors suggest that feeling unsafe might be experienced especially intensely by cyber victims in comparison to those who are bullied in a traditional way, as online aggression can occur at any day and time (Sourander et al., 2010). Research into polyvictimisation, defined as exposure to various forms of aggression including harassment, traditional and cyberbullying, has found that as polyvictimisation increased, perceptions of school safety, school equity and connectedness decreased (Garnett & Brion-Meisels, 2017).

Analyses of help-seeking behaviours among youth who experienced cyberbullying further underscores the importance of a supportive and safe school environment. A study by Schneider et al. (2015) has revealed that only one-third of cyber victims reported abuse, with the majority seeking help from a parent/non-school adult (35% for girls, 18% for boys) as compared to a school adult (20% for girls, 12% for boys). Moreover, approximately 35% of grade 7 to 9 respondents did not believe that school adults tried to stop cyberbullying when informed (Qing, 2006). It appears that addressing the school climate may not only reduce the risk of cyberbullying and traditional bullying but may also help to reduce feelings of helplessness or despair among those affected, which in turn may encourage the victims to come forward and seek help.

Further, the importance of family dynamics, specifically adequate parental supervision and interest in children's lives have been identified as protective factors against bullying behaviours, while acceptance and modelling of aggressive behaviours and harsh discipline has been associated with bullying perpetration (Pearce et al. 2011). Further, secure family environment, positive relationship between teens and their parents marked by mutual trust and communication, and family support have been identified as factors that lower the likelihood of engagement in cyberbullying perpetration among adolescents (as cited in Kowalski et al. 2018).

It goes without saying that there are certain intricacies associated specifically with cyberbullying, such as anonymity, or the fact that a great majority of teens have access to their personal computers and I-devices, which may pose a challenge for parents when aiming to supervise their children's online activities. Nonetheless, it appears that an ecological approach to cyberbullying behaviours being addressed at community, school, family and

individual levels may prove efficacious not only in drawing attention to this phenomenon, changing culture and attitudes, but also influencing individuals' behaviours.

Cyberbullying victimisation

While the protective factors associated with cyber perpetration may ultimately lead to the reduction of cyberbullying victimisation, research has found that having strong social support may protect the target from continuous online bullying and also constitute a buffer against psychological impacts of cyberbullying. A review by Allison and Bussey (2016) has found that friends of the targeted person who witness online abuse are more likely to intervene. Moreover, witnesses are also more likely to react if other passive bystanders are friends, which the authors suggest may be associated with the perception of having support (Allison & Bussey, 2016).

With regards to the effects of peer support on the outcomes of victimisation, Flaspohler, Elfstrom, Vanderzee, and Sink (2009) have found that traditional bullying victimisation is negatively associated with life satisfaction, peer and teacher support. However, the link between victimisation and poorer life satisfaction is weakened when victims perceive to have strong social support (Flaspohler et al, 2009). Research into social support in the context of cyberbullying has revealed similar effects. It has been noted that frequent family dinners, which provide an opportunity for teens and parents to connect and communicate, alleviate the negative effects of cyber victimisation on mental health and substance use among victims (Elgar et al. 2014). Parental and peer support has also been found to have a stress-buffering effect and to be related with less subjective health complaints, such as nervousness or stomach aches, often experienced by cyber victims (Fridh, Lindström, & Rosvall, 2015).

Other protective factors against cyberbullying victimisations associated with individual and environmental determinants encompass higher self-esteem, empathy, emotional intelligence, emotion regulation, and the confidence in the ability to defend oneself. School safety, positive school climate, greater satisfaction with school, residence in safer neighbourhoods have been related to lower likelihood of cyber victimisation (Kowalski et al. 2018).

Further, since anxious, insecure, and socially withdrawn students have been identified to be at an increased risk of cyber victimisation (Snakenborg et al., 2011), it appears that addressing these issues through professional counselling, taking active steps to integrate such persons with their classmates, creating opportunities for children and teens to develop nourishing friendships and providing skills to maintain them, may serve as a protective factor against potential online victimisation and its devastating consequences.

Cyberbullying bystanding

A literature review by Allison and Bussey (2016) cited a number of factors and circumstances that increase the likelihood of bystander intervention when faced with online aggression. These include modelling behaviours that disagree with and reject online aggression, witnessing disapproving reactions towards cyber aggression exhibited by other online users/non-bystanders, direct request for help expressed by the victim, being a friend of a victim or when other bystanders are friends of the victim, greater self-efficacy in the ability to assist and positive outcome expectancies. Further, empathy towards the victimised person and acceptance of diversity, such as sexuality or obesity, increase the chances of active intervention of people witnessing online aggression (for detailed discussion, see Allison & Bussey, 2016).

Theoretical basis for anti-cyberbullying programs

As can be noted from the review thus far, cyberbullying comprises complex behaviours with a number of intra- and extra-individual associations. While intra-individual factors are associated with the characteristics of specific persons, be it their gender or personality traits, extra-individual factors are associated with the broader context in which a person functions, encompassing family composition and dynamics, school climate, country laws and regulations. According to the bio-ecological framework of human development proposed by Bronfenbrenner (1997), which has been adopted by some interventions aimed to address traditional and cyber bullying, people shape and are shaped by the environment they live in. This model emphasises the interaction between an individual and the environment that has a nested structure comprising the following elements:

- microsystem – defined by the number of relationships between an individual and the individual’s immediate settings (school, family) in which the individual may fulfill different roles (student, daughter);
- mesosystem - constitutes a higher-level environment composed of interrelationships between various settings, also referred to as “a system of microsystems” (Bronfenbrenner, 1977, p.515). An individual’s mesosystem is like a sum of interactions encompassing work or school setting, family, peers, or groups they are affiliated with such as sports clubs or church;
- exosystem – this level does not contain a person, but exerts influence on the sub-systems, through specific formal or informal structures such as the government, neighbourhood, social networks;
- macrosystem – constitutes the top layer of the ecological framework and pertains to overall culture, economic, social, legal and other higher-level structures.

As suggested by Bronfenbrenner (1977), the aforementioned systems are interrelated and interdependent, and events experienced by a child in one system, may influence their functioning in another. The author illustrates that human development and thus functioning cannot be viewed in isolation from his or her immediate and broader contexts. Therefore, effecting change is best achieved by not only addressing intra-individual factors, but also by influencing the environment (and associated systems) a person is embedded in. The following section will review current knowledge on the effectiveness of cyberbullying interventions undertaken at various levels of the ecological framework.

Cyberbullying prevention and intervention programs

As cyberbullying constitutes a significant social concern, a number of countries have introduced relevant laws to regulate the behaviour. In Australia, the Criminal Code Act 1995 (Cth) stipulates that harassing and bullying someone online constitutes an offence which can see the perpetrator sentenced to three years of imprisonment or fined in excess of A\$30,000 (“Cyber-bullying,” n.d.). In the United States, 49 states have implemented anti-bullying laws (Hatzenbuehler, Schwab-Reese, Ranapurwala, Hertz, & Ramirez, 2015). A review of the effectiveness of these anti-bullying policies measured across 25 states and 59,472 students from grades 9 to 12 has revealed that students inhabiting states with anti-bullying policies

with at least one legislative component had reduced odds of reporting cyberbullying by 20% (95% CI, 9%-29%) as compared to students from states where policies did not include a relevant legislative bullying element (Hatzenbuehler et al., 2015). Moreover, this research has indicated a number of legislative aspects that had been reliably linked to the reduction of cyberbullying behaviour. These constitute compliance with anti-bullying guidelines sanctioned by the Department of Education; inclusion of the statement of scope outlining where the legislation applies and in what circumstances the school has the right to take action; descriptions of bullying behaviours; and the obligation for the local districts to develop and implement relevant policies within a set timeframe (Hatzenbuehler et al., 2015).

While regulation of cyberbullying through policies and legislations represents a macrosystem/societal approach to tackling the problem of online violence, a number of programs have also been developed on a micro, and specifically, school level (Chisholm, 2014). These programs have either been designed to prevent instances of online aggression, or to intervene in cases in which cyberbullying is already known to be occurring (Tanrikulu, 2018), or both.

According to a taxonomy proposed by Cantone et al. (2015), programs tackling bullying and cyberbullying can be divided into two groups. The first one are universal interventions aimed at changing the overall school climate and decreasing peer aggression that are often implemented by teaching staff and parents. Within this group are “whole school” and “multi-level” programs that intervene at multiple layers such as individual students, classrooms, schools, and parents. The second group constitute focused interventions that are designed for specific subgroups such as victims, bullies, and bystanders, thereby operating on a single level of action (Cantone et al., 2015). A review of 17 interventions against bullying and cyberbullying has found that in comparison to focused interventions, universal ones tend to be more effective in the areas of improving school climate and well-being of students, and reducing negative consequences of victimisation. However, the authors noted that the long-term effects of these interventions have often dissipated at follow-up (Cantone et al. 2015).

An example of a successful program containing elements of a universal and focused approach is KiVa (Kiusaamista Vastaa “against bullying”) developed in Finland. This program is delivered in classrooms where children acquire general knowledge about

traditional and cyber aggression, learn how to best respond to it, and intervene on behalf of the victims instead of being passive bystanders. At an individual level, school staff and peers provide support to the victims, but also challenge bullies directly (Salmivalli & Poskiparta, 2012). The program's duration is approximately 20 hours and is delivered by teachers who are trained and equipped with appropriate program manual, and lesson resources. Parents receive a guide providing information about general bullying and cyberbullying (Williford et al., 2013). The randomised controlled-trial conducted by Williford et al. (2013) among children from grades 4 to 9 revealed that the odds of reporting cyber victimisation were 29% greater for students who did not receive KiVa intervention as opposed to student who did. With regards to cyberbullying, the effect of the program was most prominent for younger children ($M=11.32$), as those who did not participate in the program were 69% more likely to cyberbully others, but the intervention was ineffective for older groups ($M = 12.88$ and 14.46). This finding indicates that it is important to target anti-bullying programs to younger children in order to optimise the program's effectiveness.

Apart from KiVa, a number of other prevention and intervention programs have been developed to address online aggression. A literature review by Cioppa, Neil, and Craig (2015), examined 12 whole school programs predominantly targeting 12-13 year-olds. These programs varied in terms of aims (Internet safety skill training vs addressing cyberbullying behaviours), modes of delivery, duration and intensity, involvement of parents, teachers and wider community. Only five out of 12 studies reported lower incidence of victimisation, whilst six out of 12 demonstrated a decrease in cyberbullying perpetration. Although the programs targeted cognitive, behavioural and social variables in line with evidence-based risk and protective factors, variability in scientific merit associated with the measurement of these interventions have prevented the authors from providing program recommendations (Cioppa et al., 2015)

A review of the interventions that involve the use of information and communication technologies (ICTs) has revealed that only two (No Trap! and KiVa) out of nine studies relevant to cyberbullying have demonstrated effectiveness in reducing victimisation and perpetration rates (Nocentini, Zambuto, & Menesini, 2015). Similarly to Cioppa's et al. (2015) research, the effectiveness of the majority of interventions has proven hard to establish as some programs did not include control groups and adequate follow-up measurements, or provided limited information on outcomes achieved.

Most recent evaluations of cyberbullying interventions, however, have identified a number of specific program components that have been found to decrease cyberbullying. These include parent education, communication and social skills training in online and offline settings, empathy training and the ability to perceive the situation from the standpoint of persons involved, coping skills through teaching youth strategies they can implement to cope with online aggression, and digital citizenship defined as a responsible use of technology (Hutson, Kelly, & Militello, 2018). Surprisingly, changing attitudes towards cyberbullying and improving youth's self-efficacy have decreased cyberbullying or cybervictimisation in only three out of seven studies and two out of four studies respectively (Hutson et al. 2018).

A review of prevention and intervention cyberbullying programs published before August 2016 and aimed at students between the ages of 11 and 19 has found a high rate of success (Tanrikulu, 2018). Seventeen interventions have been evaluated that differed in duration, intensity of sessions, theoretical background, use of technology, and all except one had achieved positive outcomes in terms of reduction and prevention of cyberbullying behaviours. Due to considerable variability in program characteristics, establishing a pattern of common components has been challenging. However, Tanrikulu (2018) has noted that programs of various duration (from one day to over a year) have been equally successful along with these that have targeted traditional bullying as well.

Cyberbullying prevention/intervention programs and associated challenges

One of the challenges associated with delineating and identifying common features of successful cyberbullying programs is based on the level of quality of studies that had reviewed their efficacy. The quality of such information is of paramount importance as it strengthens the confidence among the decision-makers and program facilitators that the success of a given approach is grounded in solid and evidence-based research. Cioppa et al. (2015) has provided a list of recommendations pertaining to the evaluation and systematic implementation of various interventions. These encompass adequate study design (experimental or quasi-experimental), data collection at baseline with a follow-up procedure at 6 and 24 months in order to investigate the long-term effects of interventions, and

gathering data from multiple sources of information, such as students, teachers, and parents (Cioppa et al., 2015).

Adequate implementation of the cyberbullying program also constitutes an important issue as it ensures internal validity, i.e. the confidence that outcomes are achieved as a result of an intervention rather than other factors (Tanrikulu, 2018). A review of 17 studies by Tanrikulu (2018) has indicated that only three provided information on treatment integrity pertaining to implementation of the program as it was intended. To address this problem, Cioppa et al. (2015) have recommended that cyberbullying programs are provided with standardised training manual (published manual, website or a trained facilitator), assessment tools and adequate monitoring, support for program facilitators and staff training, as well as allow flexibility to adjust the programs to meet schools' objectives, and contain information on program maintenance and costs.

Another issue associated with some of the cyberbullying prevention and intervention is associated with the specification of a theoretical approach underlying specific programs. As noted in a review by Tanrikulu (2018), information on the theoretical approaches used in the intervention studies has not been sufficiently detailed or indicated at all. According to the author, each program should contain such information as it assists educators with understanding the mechanism through which cyberbullying will be addressed and will also allow researchers to examine the effectiveness of a given approach (Tanrikulu, 2018).

In addition to the aforementioned points, Hutson et al. (2018) has recommended the inclusion of a cyberbullying definition to ensure that the studies measure the same construct and consideration of cultural context that may affect intervention outcomes. Further, Tanrikulu (2018) has called for the establishment of a valid and reliable instrument that could be used in all future research, as currently studies implement measurement tools of variable psychometric properties. Such an approach would ensure that all studies are measuring the same concept and would allow for direct program comparisons.

Although the establishment of a uniform definition of cyberbullying or a measurement tool may prove challenging and not achievable for years to come, Kowalski et al. (2014) have recommended that the accuracy of cyberbullying victimisation and perpetration can be maximised through the use of multiple-item measurement tools compared

to single-item instruments. Moreover, following moderator analyses, the accuracy of estimates tends to be improved when the definition of cyberbullying behaviours or the word “bully” is provided and when traditional bullying (victimisation and perpetration) is measured as well (Kowalski et al. 2014).

Gaps in the literature and recommendations for future research

As can be noted from the discussion above, cyberbullying prevention and intervention programs are evaluated with a varying degree of scientific rigor, which poses a great challenge to the identification of specific program characteristics that contribute to its success or failure. Therefore, future research on the effectiveness of cyberbullying programs should ensure a high degree of scientific merit so that recommendations for future prevention and interventions can be provided.

Further, one of the aspects that makes cyberbullying a unique phenomenon is the use of technology. Notably, in a review by Tanrikulu (2018), only four programs made use of technology to address cyberbullying. Also, a number of studies investigating the effectiveness of ICTs against traditional and cyber bullying provide incomplete data or the methodology used for their evaluation does not allow causal inferences (Nocentini et al., 2015). Future research should therefore aim to establish the value and unique contributions of ICTs in prevention and intervention programs.

The majority of prevention and intervention programs are delivered by school staff and on school grounds, yet relatively little is known on the effectiveness of programs delivered outside of the school setting and by members of community compared to school staff. As children and youth operate in a variety of microsystems, with school being only one of them, the development and investigation into the effectiveness of community anti-cyberbullying programs is warranted.

Youth with disabilities and chronic conditions, such as ADHD, are at an increased risk of cyber victimisation. However, little is known whether current intervention and prevention programs have a similar effect on this population as compared to healthy/typically developing children. Future research into this area could establish success rates of the

programs, establish components that work well, and provide recommendations that could maximise positive outcomes among this group.

Finally, the majority of programs evaluated in current review has been predominantly addressed to teenagers. Yet, research shows that 55% of children between 3-4 years and 67% of 5-7 year-olds use tablets, and 16% and 32% of these groups respectively own their personal tablets (Ofcom, 2016). It may be that early introduction of age-appropriate cyberbullying prevention programs could reduce rates of future victimisation and perpetration. A longitudinal study design could address this gap in the literature.

Study limitations

The current executive summary provides an overview of the deluge of information pertaining to cyberbullying prevalence, associated risk and protective factors, as well as cyberbullying prevention and intervention programs. However, the scope of the review was limited to literature searches through Ebsco Host databases and Google Scholar. Therefore, future research should encompass other search platforms and extend to grey literature.

Moreover, the majority of research on the effectiveness of cyberbullying programs is descriptive in nature. A statistical approach to measuring the pooled effectiveness of these approaches, through meta-analytic reviews, could improve the accuracy of estimates, identify inconsistencies and sources of variability.

Conclusions

Cyberbullying constitutes a prevalent form of online peer aggression linked to a plethora of psychological, behavioural and social problems. The variables associated with the risk factors for cyberbullying perpetration, victimisation, and cyber by-standing among adolescents are numerous, and thus require attention on multiple levels of human functioning. This review has indicated that laws introduced at a macrosystem level are effective in decreasing cyberbullying. Prevention and intervention programs that target whole-school environment, involve parents, teachers, and students, thereby engaging all levels of the environment in which teens develop, also tend to decrease cyberbullying perpetration, victimisation and bystanding.

The current review has also described challenges associated with the measurement of effectiveness of cyberbullying prevention and intervention programs and provided recommendations on how these could be avoided in future. A number of gaps in the current knowledge have been identified including a scarcity of cyberbullying community-based programs delivered by non-school staff and a paucity of knowledge regarding their effectiveness. Future research should consider exploration of cyberbullying prevention and intervention programs within local communities as they may also prove successful with regards to changing the culture around cyberbullying, thereby decreasing instances of peer online aggression.

References

- Allison, K. R., & Bussey, K. (2016). Cyber-bystanding in context: A review of the literature on witnesses' responses to cyberbullying. *Children and Youth Services Review, 65*, 183-194. Retrieved from <http://dx.doi.org/10.1016/j.chidyouth.2016.03.026>
- Australian Bureau of Statistics (2018). Household use of information technology, Australia 2016-17. Retrieved from <http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0>
- Bandura, A. (1990). Selective activation and disengagement of moral control. *Journal of Social Issues, 46*(1), 27–46. Retrieved from <https://doi.org/10.1111/j.1540-4560.1990.tb00270.x>
- Barlett, C. P., & Chamberlin, K. (2017). Examining cyberbullying across the lifespan. *Computers in Human Behavior, 17*, 444-449. Retrieved from <http://dx.doi.org/10.1016/j.chb.2017.02.009>
- Bronfenbrenner, U. (1977). Toward an experimental ecology of human development. *American Psychologist, 32*(7), 513-531. Retrieved from <http://dx.doi.org/10.1037/0003-066X.32.7.513>
- Cantone, E., Piras, A. P., Vellante, M., Preti, A., Daníelsdóttir, S., D'Aloja, E., Lesinskiene, S., Angermeyer, M. C., Carta, M. G., & Bhugra, D. (2015). Intervention on bullying and cyberbullying in schools: A systematic review. *Clinical Practice and Epidemiology in Mental Health, 11*(Suppl. 1: M4), 58-76. doi: 10.2174/1745017901511010058
- Chisholm, J. F. (2014). Review of the status of cyberbullying and cyberbullying prevention. *Journal of Information Systems Education, 25*(1), 77-87. Retrieved from <http://jise.org/Volume25/n1/JISEv25n1p77.html>
- Cioppa, V. D., O'Neil, A., & Craig, W. (2015). Learning from traditional bullying interventions: A review of research on cyberbullying and best practice. *Aggression and Violent Behavior, 23*, 61-68. Retrieved from <https://doi.org/10.1016/j.avb.2015.05.009>
- Cyber-bullying. (n.d.) Retrieved from <https://www.acorn.gov.au/learn-about-cybercrime/cyber-bullying>
- Dooley, J. J., Pyzalski, J., & Cross, D. (2009). Cyberbullying versus face-to-face bullying. A theoretical and conceptual review. *Journal of Psychology, 217*(4), 182–188. doi: 10.1027/0044-3409.217.4.182

- Elgar, F. J., Napoletano, A., Saul, G., Dirks, M. A., Craig, W., Poteat, V. P., Holt, M., & Koenig, B. (2014). Cyberbullying victimization and mental health in adolescents and the moderating role of family dinners. *JAMA Pediatrics*, *168*(11), 1015-1022. Doi: 10.1001/jamapediatrics.2014.1223
- Fridh, M., Lindström, M., & Rosvall, M. (2015). Subjective health complaints in adolescent victims of cyber harassment: moderation through support from parents/friends - a Swedish population-based study. *BMC Public Health*, *15*, 949. Doi: 10.1186/s12889-015-2239-7
- Flaspohler, P. D., Elfstrom, J. L., Vanderzee, K. L., & Sink, H. E. (2009). Stand by me: The effects of peer and teacher support in mitigating the impact of bullying on quality of life. *Psychology in the Schools*, *46*(7), 636-649. Doi: 10.1002/pits.20404
- Garnett, B. R., & Brion-Meisels, G. (2017). Intersections of victimization among middle and high school youth: Associations between polyvictimization and school climate.
- Hatzenbuehler, M. L., Schwab-Reese, L., Ranapurwala, S. I., Hertz M. F., & Ramirez, M. R. (2015). Associations between anti-bullying policies and bullying in 25 states. *JAMA Pediatrics*, *169*(10):e152411. doi:10.1001/jamapediatrics.2015.2411
- Hong, J. S., & Espelage, D. L. (2012). A review of research on bullying and peer victimization in school: An ecological system analysis. *Aggression and Violent Behavior*, *17*(4), 311–322. Retrieved from <http://dx.doi.org/10.1016/j.avb.2012.03.003>.
- Hutson, E., Kelly, S., & Militello, L. K. (2018). Systematic review of cyberbullying interventions for youth and parents with implications for evidence-based practice. *Worldviews on Evidence-Based Nursing*, *15*(1), 72–79. doi:10.1111/wvn.12257
- Juvonen, J., & Graham, S. (2014). Bullying in schools: The power of bullies and the plight of victims. *Annual Review of Psychology*, *65*, 159-185. doi:10.1146/annurev-psych-010213-115030
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin* *140*(4), 1073-1137. doi:10.1037/a0035618
- Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). Current research on cyberbullying. In *Cyberbullying: Bullying in the Digital Age*, (2nd ed.), (pp. 89-117). Chichester, Wiley-Blackwell.
- Kowalski, R.M., Limber, S. P., & McCord, A. (2018). A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior*, *1-13*. Retrieved from <https://doi.org/10.1016/j.avb.2018.02.009>

- Langos, C. (2012). Cyberbullying: The challenge to define. *Cyberpsychology, Behavior, and Social Networking*, 15(6), 285-289. doi:10.1089/cyber.2011.0588
- Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, K., & Rainie, L. (2011). Teens, kindness and cruelty on social network sites. Washington, DC: Pew Research Centre.
- Mason, K. L. (2008). Cyberbullying: A preliminary assessment for school personnel. *Psychology in the Schools*, 45(4), 323-348. Doi: 10.1002/pits.20301
- Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., & Menesini, E. (2010). Cyberbullying: Labels, Behaviours and Definition in Three European Countries. *Australian Journal of Guidance and Counselling*, 20(2), 129-142. Retrieved from <https://doi.org/10.1375/ajgc.20.2.129>
- Notar, C. E., Padgett, S., & Roden, J. (2013). Cyberbullying: Resources for intervention and prevention. *Universal Journal of Educational Research*, 1(3), 133-145. doi: 10.13189/ujer.2013.010301
- Ofcom (2016). Children and parents: media use and attitudes report 2016. United Kingdom. Retrieved from <https://www.ofcom.org.uk/research-and-data/media-literacy-research/children/children-parents-nov16>.
- Olweus, D. (1993). *Bullying at school: What we know and what we can do*. Oxford: Blackwell.
- Patchin, J.W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, 4(2), 148-169. doi: 10.1177/1541204006286288
- Pearce, N., Cross, D., Monks, H., Waters, S., & Falconer, S. (2011). Current evidence of best practice in whole-school bullying intervention and its potential to inform cyberbullying interventions. *Australian Journal of Guidance and Counselling*, 21(1), 1-21. doi: 10.1375/ajgc.21.1.1
- Qing, L. (2006). Cyberbullying in schools: A research of gender differences. *School Psychology International*, 27(2), 157-170. doi:10.1177/0143034306064547
- Roy Morgan Research. (2016). *9 in 10 Aussie teens now have a mobile (and most are already on to their second or subsequent handset)*[Press release]. Retrieved from <http://www.roymorgan.com/findings/6929-australian-teenagers-and-their-mobile-phones-june-2016-201608220922>
- Salmivalli, C., & Poskiparta, E. (2012). Making bullying prevention a priority in Finnish schools: The KiVa antibullying program. *New Directions for Youth Development*, 2012(133), 41-53. doi:10.1002=yd.20006

- Schneider, S. K., O'Donnell, L., & Smith, E. (2015). Trends in cyberbullying and school bullying victimization in a regional census of high school students, 2006-2012. *Journal of School Health, 85*(9), 611-620. Retrieved from <https://doi-org.ezproxy-f.deakin.edu.au/10.1111/josh.12290>
- Slonje, R. & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology, 49*, 147–154. doi: 10.1111/j.1467-9450.2007.00611.x
- Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49*(4), 376–385. doi:10.1111/j.1469-7610.2007.01846.x
- Snell, P. A., & Englander, E. (2010). Cyberbullying victimization and behaviors among girls: Applying research findings in the field. *Journal of Social Sciences, 6*(4), 510-514. Retrieved from <https://doi.org/10.3844/jssp.2010.510.514>
- Sourander, A., Brunstein Klomek, A., Ikonen, M, Lindroos, J., Luntamo, T., Koskelainen, M; Ristkari, T, & Helenius, H. (2010). Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study. *Arch Gen Psychiatry, 67*(7), 720-728. doi:10.1001/archgenpsychiatry.2010.79
- Spears, B. A., Taddeo, C. M., Daly, A. L., Stretton, A., & Karklins, L. T. (2015). Cyberbullying, help-seeking and mental health in young Australians: implications for public health. *International Journal of Public Health, 60*(2), 219–226. Retrieved from <https://doi-org.ezproxy-f.deakin.edu.au/10.1007/s00038-014-0642-y>
- Tanrikulu, I. (2018). Cyberbullying prevention and intervention programs in schools: A systematic review. *School Psychology International, 39*(1), 74-91. doi: 10.1177/0143034317745721
- van Geel, M., Vedder, P., & Tanilon, J. (2014). Relationship between peer victimization, cyberbullying, and suicide in children and adolescents. A meta-analysis. *JAMA Pediatrics 168*(5), 435-442. doi:10.1001/jamapediatrics.2013.4143
- Walrave, M. & Heirman, W. (2011). Cyberbullying: Predicting victimisation and perpetration. *Children & Society Volume, 25*, 59–72. doi:10.1111/j.1099-0860.2009.00260.x
- Willard, N.E. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Retrieved from <http://books.google.com>

Williford, A., Elledge, L. C., Boulton, A. J., DePaolis, K. J., Little, T. D., & Salmivalli, C. (2013) Effects of the KiVa antibullying program on cyberbullying and cybervictimization frequency among Finnish youth. *Journal of Clinical Child & Adolescent Psychology*, 42(6), 820-833. doi:10.1080/15374416.2013.787623

Ybarra, M. L., & Mitchell, K. J. (2004). Youth engaging in online harassment: associations with caregiver–child relationships, Internet use, and personal characteristics. *Journal of Adolescence*, 27, 319–336. Retrieved from <http://www.unh.edu/ccrc/pdf/jvq/CV63.pdf>