Cyberbullying: Concepts, theories, and correlates informing evidence-based best practices for prevention

Nadia S. Ansary

Rider University, United States of America

ARTICLE INFO

Keywords:
Cyberbullying
Cybervictimization
Electronic bullying
Prevention
Intervention

ABSTRACT

Emerging evidence has revealed that many characteristics of cyberbullying—its definition, prevalence rates, risk and protective factors, outcomes, and prevention strategies—are related and yet somewhat distinct from traditional bullying. The ubiquity of technology in the lives of youth presents an opportunity for individuals to intentionally and repetitively harm others, 24 h per day, sometimes with complete anonymity, and often without consequence. This is concerning given the high rates of psychopathology associated with cybervictimization, over and above, traditional bullying. Given the current state of the field, this literature review provides a critical synthesis of the extant knowledge concerning (1) a definition of cyberbullying; (2) theories explaining cyberbullying; (3) prevalence rates; (4) a brief developmentally-focused overview of adolescents and their online use; (5) risk and protective factors; (6) negative psycho-social outcomes, over and above traditional bullying; and (7) a brief overview of prevention and intervention programming with information for key stakeholders. Implications and future directions are discussed.

While some researchers view cyberbullying as not profoundly distinct from traditional bullying (Olweus & Limber, 2018; see Vaillancourt, Faris, & Mishna, 2017), the nuanced differences between the two suggest that generalizing findings from traditional bullying to cyberbullying may be inadequate (Savage & Tokunaga, 2017). Growing evidence reveals that many facets of cyberbullying—from its definition, prevalence rates, risk and protective factors, outcomes, and prevention strategies—are related and yet somewhat distinct from traditional bullying (Espelage & Hong, 2017; Kowalski, Limber, & McCord, 2019; Patchin & Hinduja, 2012; Smith et al., 2008; Vaillancourt et al., 2017; Zych, Farrington, & Ttofi, 2019). Cyberspace makes bullying easier, more accessible, and inflicts greater harm than traditional bullying (see Vaillancourt et al., 2017 for a review).

Cumulatively, these factors suggest that cyberbullying may be more complex and more insidious than traditional bullying. And yet, the cyberbullying literature is still nascent with advancements in theory and empirical evidence required to fuel developments in prevention and intervention programming. A call-to-action is necessary given several factors. First, findings from the Pew Research Center suggest that 95% of teens own or have access to a smartphone and 45% of teens surveyed report being “online on a near-constant basis” (Anderson & Jiang, 2018). Twenty-four percent of youth surveyed by Pew felt that social media is the reason for greater bullying and rumor spreading (Anderson & Jiang, 2018). Second, mounting evidence exists on the long-term negative outcomes uniquely associated with cyberbullying (Fahy et al., 2016; Vaillancourt et al., 2017) which is particularly troubling in light of the fact that roughly one in five adolescents experience it (Hinduja & Patchin, n.d.; Selkie, Fales, & Moreno, 2016). Vaillancourt et al. (2017) highlight that over and above traditional bullying, cyberbullying is uniquely associated with (a) somatic difficulties (e.g., headaches, stomach aches, etc.); (b) depression; (c) suicidal ideation and suicide attempts; (d) symptoms of Post-Traumatic Stress Disorder (PTSD); and (e) academic difficulties, among others.

Given the current state of the field, this literature review provides a critical synthesis of the extant knowledge concerning (1) a definition of cyberbullying; (2) theories explaining cyberbullying; (3) prevalence rates; (4) a brief developmentally-focused overview of adolescents and their online use; (5) risk and protective factors; (6) outcomes, over and above traditional bullying; and (7) a brief overview of prevention and intervention programming with information for key stakeholders. In order to conduct this review, a literature search of the most current scholarship published in peer-reviewed outlets from 2010 and beyond was conducted. Keyword searches included cyberbullying, cybervictimization, electronic bullying, online bullying, and technology and bullying. Only English language publications were used. Reports from large-scale
studies by government agencies and evidence-based advocacy groups were also included. Furthermore, this review mainly focuses on adolescents who are defined “as individuals in the 10–19 years age group” (World Health Organization [WHO], 2013). Consistent with that definition, in this paper the term adolescent generally refers to middle- to high-school-aged individuals who are distinct from college-aged samples.

In terms of the framework guiding this literature synthesis, developmental psychopathology provides a research-to-application continuum which is most useful in addressing this problem. Briefly, as a discipline, developmental psychopathology explores the intersection of human development (e.g., exploring change that recognizes the individual as an active agent in his or her development) and clinical psychology (e.g., concerned with the diagnosis and treatment of disordered behavior) with a specific focus on using research to inform prevention strategies (Hinshaw, 2013). Many scholars recognize that developmentally-focused social-ecological frameworks that view bullying as a dynamic process involving many levels of influence (e.g., family, school, neighborhood) are most useful in explaining bullying (Swearengin & Hymel, 2015; Zych et al., 2019). Furthermore, recent evidence parsing risk and protective factors uniquely associated with cyberbullying are also helpful in conceptualizing the issue within a developmental psychopathology framework (Kowalski et al., 2019; Zych et al., 2019). To date, no literature exists examining cyberbullying through this lens, leaving a void in the scholarship and evidence-based recommendations for best practices to address cyberbullying.

1. Operational definition

Failure to have a consensus about a definition is not a trivial problem. It is especially noteworthy that many researchers vary in how they operationally define cyberbullying and this necessarily has implications for the rigor of its study and for prevention programming. How can adequate cyberbullying prevention strategies be effectively designed when the definition and scope of the problem remain a moving target?

There are two characteristics of cyberspace that present challenges to the existing definition of traditional bullying which requires: an intent to harm, a power imbalance, and repetition of the harmful behavior (Olweus, 1999). First, many have argued that the power imbalance criteria—either with regard to physical or social power required in the traditional bullying definition—is less explicit in the online context. Cyberspace inherently contributes to a power imbalance: the disinhibition effect affords online users opportunities to behave more brazenly (Suler, 2004), and to attack with anonymity (Hinduja & Patchin, 2015a; see also Peter & Petermann, 2018). Another contributor to the power imbalance is the fact that a single malicious act may be repeatedly disseminated and viewed by multiple users: This also negates the intentional repetition criteria within the traditional bullying definition (Hinduja & Patchin, 2015a; see also Peter & Petermann, 2018).

Some researchers have attempted to sidestep this dilemma by simply using global measures of cyberaggression (i.e., asking about cybervictimization without any inquiry about repetition) as indicators of cyberbullying (Kowalski et al., 2019; Peter & Petermann, 2018). The implications of this are two-fold: operationalizing cyberaggression as synonymous with cyberagression has compromised the internal validity of those studies, and it has also obfuscated a clear understanding of prevalence rates. For example, in their review of the literature, Hinduja and Patchin (n.d.) found victimization rates that ranged from 0.4% to 92% and offending values ranged from 1.0% to 60.4%. Similarly, vast prevalence rates have been reported in other large-scale reviews of the cyberbullying literature (Kowalski et al., 2019; Selkies et al., 2016). Beyond failure to make a distinction between cyberaggression and cyberbullying, other reasons for this vast range of prevalence rates include (1) the time parameter used in measurement (i.e., how many times has this happened in the last 30 days or in the last year?, etc.); (2) age of participants (since cyberbullying during elementary school is generally low but increases in adolescence; see Kowalski et al., 2019); (3) whether a single item or multiple items were used (with multiple item measures showing higher validity); and (4) cross-country comparisons where there may be differences in the availability of technology (Kowalski et al., 2019; Whitaker & Kowalski, 2015).

In an important contribution to the field, Peter and Petermann (2018) distilled the essential elements of existing cyberbullying definitions in their concept analysis of articles published since 2010. Their findings led to the following definition of cyberbullying as “using information and communication technologies (ICT) to repeatedly and intentionally harm, harass, hurt and/or embarrass a target” (p. 359). This definition is not significantly different than earlier forms which are most often cited in the literature: Smith et al. (2008) define cyberbullying as “an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself” (p. 376); and Hinduja and Patchin (n.d.) define it as “… when someone repeatedly and intentionally harasses, mistreats, or makes fun of another person online or while using cell phones or other electronic devices”. Cumulatively, these nearly identical definitions reveal that a consensus has developed.

2. Theoretical models

Similar to the lack of agreement about a cyberbullying definition, there is no consensus about a comprehensive theoretical model that explains cyberbullying. The largely a-theoretical state of the cyberbullying literature has provided a barrier to a holistic understanding of the issue (Kowalski, Glumeti, Schroeder, & Lattanner, 2014). Only one theoretical model, to date—the Barlett and Gentile cyberbullying model (BGCM, Barlett, 2017)—explicitly examines cyberbullying perpetration. Most scholars examining cyberbullying have adapted models of aggression, such as the general aggression model (Anderson & Bushman, 2002; see Barlett, 2017; Savage & Tokunaga, 2017), and the (I-cubed) theory (Slotter & Finkel, 2011; see Wong, Cheung, & Xiao, 2018). Beyond explicit aggression models, the social-ecological diathesis-stress model has been used to explain bullying (Swearengin & Hymel, 2015) and likely has great utility in explaining cyberbullying. Each of these models will be briefly evaluated.

The Barlett and Gentile cyberbullying model (BGCM, Barlett, 2017) accounts for (1) anonymity in cyberspace; (2) the recognition that one's physical size does not contribute to a power imbalance online; and (3) both of these mediate positive attitudes towards bullying, ultimately predicting to cyberbullying perpetration. While the model has been supported in examinations by its creators (Barlett, 2017; Barlett, Madison, Heath, & DeWitt, 2019), there are several issues with its usefulness. First, the theory is too simplistic given that it ignores prior victimization as a catalyst for online perpetration of bullying which has been found to be a significant correlate of cyberbullying (Kowalski et al., 2014; Kowalski et al., 2019; Waasdorp & Bradshaw, 2015; see also Wong et al., 2018). Second, person-specific factors (e.g., self-control, moral disengagement, use of technology, etc.) and context-specific factors (e.g., parental factors including monitoring of technology, schools failing to have explicit policies on consequences for cyber-attacks, etc.) that have been found to be uniquely associated with cyberbullying perpetration (Kowalski et al., 2019; Zych et al., 2019), are not represented in the model. Third, the operational definition of the construct belief in the irrelevance of muscularity during online bullying (Bi-MOB) has several issues, namely, (a) it is ambiguous, (b) careful consideration of the items reveals they not only assess the belief that 'size does not matter' online but concurrently assess the individual's positive attitudes towards cyberbullying which is another unique predictor in the model, and (c) the scale has shown varied reliability with reported alpha levels ranging from as low as 0.52 to greater than 0.69 (Barlett et al., 2019). Most importantly, the model has been examined only with
adult samples ages 19–74 (Barlett et al., 2019), solely uses online data collection procedures, and has been empirically examined only by its creators.

Other models that have shown some utility in explaining cyberbullying are based on adapted versions of the generalized aggression model (Anderson & Bushman, 2002) which examines person-specific factors (e.g., demographic variables, personality, etc.) in confluence with situation-specific factors (e.g., presence of bystanders, school climate, etc.) (Kowalski et al., 2014; Savage & Tokunaga, 2017). In applying this model, Savage and Tokunaga (2017) found that rather than a direct relationship between person-specific predictors and cyberbullying as an outcome, the relationship is much more complex and dynamic. In that study, high cyberbullying perpetration was demonstrated among two sets of individuals (1) one who were rated high on internet self-efficacy, low on verbal aggressiveness, and high on social skills; and (2) ones who were rated high on internet self-efficacy, high on verbal aggressiveness, and low on social skills. These interactions suggest that a confluence of many factors is at play in explaining cyberbullying since no one factor universally predicted to the outcome. Moreover, the findings suggest that extension of traditional bullying models to explain cyberbullying are inadequate (Savage & Tokunaga, 2017).

I^3 (I-cubed) theory (Slottet & Finkel, 2011), developed to explicate intimate partner violence, has been adapted by Wong et al. (2018) to examine cyberbullying perpetration. I^3 theory examines predictors—both at the individual and situational level of—instantiation (i.e., factors that provoke aggression), impellence (i.e., factors that promote cyberbullying), and inhibition (factors that reduce the likelihood of cyberbullying perpetration). While the model demonstrated explanatory power, it requires replication with younger samples in the West since the sample under investigation was Hong Kong undergraduates (Wong et al., 2018). Furthermore, the authors use a broader definition of cyberagression (e.g., receiving messages that are harmful but with no indication as to whether these happened repeatedly or not) and thus replication with a more stringent measurement of cyberbullying is necessary.

In contrast to these models of aggression, Swearer and Hymel's (2015) social-ecological diathesis-stress model provides a complex framework that recognizes the dynamic interplay of genetics, social, and environmental factors in explaining bullying perpetration. The model accounts for how various settings (e.g., family, school, neighborhood) in a child's life can interact with the child's genetic vulnerabilities (e.g., temperament, personality, etc.), and individual risk and protective factors to explain bullying involvement. Importantly, from a developmental psychopathology framework, the model accounts for a dynamic interplay of genetic vulnerability, environmental stressors, and the norms of environmental contexts such as school, in explaining involvement in bullying. Because of its complexity, the social-ecological diathesis-stress model provides a way to integrate the empirical evidence on the issue in a holistic model. Although the model was proposed specifically for traditional bullying, it has power when considering cyberbullying. Consider the following factors, all represented in this explanatory model, (a) a child's propensity to aggress (e.g., genetic vulnerability, moral disengagement; etc.); (b) prior experiences with being bullied (environmental stressors); (c) moderating factors related to cyberspace (e.g., strength of the disinhibition effect and one's technological efficacy); and (d) parental factors (e.g., parent-child relationships and monitoring of technology which are context-specific factors).

While the models noted here possess strengths in explaining cyberbullying perpetration, many require modification to sufficiently capture its complexity. Adequate representation of personal, familial, school, peer, and neighborhood/community contexts, as well as the most current set of risk and protective factors examined in the literature are lacking in the extant models. Accordingly, incorporating all of these elements is critical in the refinement of existing models and in the development of new ones.

3. Prevalence

A common yet concerning issue in the cyberbullying literature is the wide range of prevalence rates. This variability has been largely due to discrepancies in operationally defining and measuring cyberbullying in a way that discriminates it from cyberaggression. Nonetheless, large scale studies and reviews place the average annual cybervictimization rates between 14%–21%. The U.S. Department of Health and Human Services, Centers for Disease Control report that 14.9% of high schoolers reported being cyberbullied in the last year (Kann, McManus, Harris, & et al., 2018). Hinduja and Patchin (n.d.) conducted an extensive review of the literature (evaluating over 234 scholarly publications) and found a wide range of rates with the average lifetime incidence rate of cybervictimization at 21% and 13% for cyberbullying perpetration. These values are generally consistent with other data on the incidence of cyberbullying (Kowalski et al., 2019; Olweus & Limber, 2018; Selkie et al., 2016).

4. Adolescents and apps

The pace of emerging technology that draws in a young population of users creates challenges for the scholarly study of cyberbullying. Social media applications (Apps) create increasingly sophisticated yet easy-to-use modalities for youth to connect to one another in both helpful and harmful ways. Suicides of young adolescents as a result of cyberbullying have fueled a more urgent dialogue concerning the role of social media Apps—such as Ask.fm and Kik—in cyberbullying (Smith-Spark, 2013; Wallace, 2015). These—as well as other free Apps such as Voner, Whisper, Whir, Rum—allow users to anonymously post photos or messages that can be viewed for a short time online. Others like Snapchat allow users to post privately or publicly to subsets of friends. Likewise, fake accounts on Facebook, Instagram, and Twitter also afford the opportunity to anonymously engage in cyberbullying perpetration. Although, most social media platforms require a minimum user age of 13, many Apps are used by younger youth (see Valencia, 2014).

Emerging evidence suggests that there are age differences in the ways that individuals engage social media to cyberbully. For elementary school-aged youth, online gaming (which affords users the ability to converse via headset as well as in-game text) has been identified as the most widespread way to engage in cyberbullying (see Kowalski et al., 2019). Among adolescents, cyberbullying most commonly occurs via social media (Kowalski et al., 2019) with one study identifying Twitter and Facebook as the most commonly used social media platforms to do so (Whittaker & Kowalski, 2015). Within a small young adult sample, both public and private comments, status updates, and posts, were the most common ways of engaging in cyberbullying (Brody & Vangelisti, 2017).

School-aged social media users are an at-risk population for cyberbullying involvement. First, school-aged youth have nascent emotional and cognitive regulatory systems in the brain, which govern behavior. More specifically, the prefrontal cortex of the brain—which administers impulse control, judgment, and thinking through anticipated consequences of one's behavior—does not conclude development until young adulthood (Pharo, Sim, Graham, Gross, & Hayne, 2011). Second, some features of cyberspace—anonymity, ubiquity of technology, and short time-duration of posts—afford opportunities for youth with an intention to harm others to do so with deleterious consequences for the target (Peter & Petermann, 2018; Wong et al., 2018; Zych et al., 2019). To illustrate, the individual who bullies may be a complete stranger or someone the target knows who is posting anonymously (or alternatively using an alias or different identity) which can contribute to the target feeling helpless. Moreover, the attacks may be occurring privately or publicly and the target may receive posts that are viewable for an extremely short time (just a few seconds) or for much longer periods of time as well as re-posted easily. Thus, cyberbullying incidents can be privy to a potentially large online audience of peers and strangers.
leaving targets unsure of who has “seen” the incident (e.g., photo, obscene posting, etc.). Third, the frequency of cyberbullying intervention is quite low: Adults are not typically present online and evidence suggests that nearly 91% of bystanders report that they did nothing when they witnessed such an attack (Lenhart et al., 2011). Fourth, reporting of cyberbullying incidence is very low since targets may fear parents revoking their access to technology in order to protect them from further abuse. The confluence of low adult supervision, the perception that cyberbullying will not be reported, low bystander intervention, and the lack of repercussions for such behavior are all potent contributors to cyberbullying perpetration (Kowalski et al., 2019; Zych et al., 2019).

Cumulatively, the factors presented in this section provide the backdrop for cyberbullying involvement. The convergence of these factors sets the stage for targets experiencing helplessness, psychological distress, as well as fear that there is no safe place online (Dehue, 2013; Vandebosch & Van Cleemput, 2009). From this perspective, it is clear why cyberbullying involvement is associated with long-term psycho-social dysfunction, above and beyond the effects seen for traditional bullying.

5. Risk and protective factors

Recent years have seen an increase in the identification of risk and protective factors of cyberbullying, and of course, many of these are shared with traditional bullying. Two reviews on this issue, Kowalski et al. (2019) and Zych et al. (2019), are particularly rigorous in their focus on the unique risk and protective factors of cyberbullying. The realms of risk and protective factors identified in those reviews relate to the domains seen in Swearer & Hymel’s social-ecological diathesis-stress model (Swearer & Hymel, 2015), namely, individual, family, peer, school, and community. Before proceeding through the list of risk and protective factors, it is important to point out that in a review of meta-analyses considering protective factors on this issue (Zych et al., 2019), the protective factors for cybervictimization with the strongest effect size were those at the individual level related to personal competencies and low technology use, while for cyberbullying perpetration, the strongest protective effects were found for low technology use and peer-level factors. It is also critical to note that no prospective longitudinal studies have been conducted to identify risk and protective factors of cyberbullying, and existing findings are mainly garnered from cross-sectional designs (Zych et al., 2019).

For cyberbullying victimization, individual-level risk factors include: low self-esteem, self-control, social intelligence, low empathy, high levels of anxiety, aggression, moral disengagement, and being a victim of traditional bullying victimization (Kowalski et al., 2019). Stress and suicidal ideation have also been identified as risks for cybervictimization (Kowalski et al., 2014). Protective factors of cyberbullying victimization include high self-esteem (Kowalski et al., 2019) as well as high levels of emotional management, self-concept, and social competence (Zych et al., 2019). With regard to technology use, low levels have been found to be protective (Zych et al., 2019) while high levels are a risk (Kowalski et al., 2019). In the parenting domain, risks include a single-family household, negative family environment, and sexual abuse (Kowalski et al., 2019), while protective factors consist of parental support and warmth (Kowalski et al., 2019) and high socioeconomic status (Zych et al., 2019). Just as low peer support has been identified as a risk for cybervictimization (Kowalski et al., 2019), high peer support and positive peer interactions have been identified as a protective influence (Zych et al., 2019). School and community factors also play a role in that school climate, safety, satisfaction with school, and a safe neighborhood have been identified in these two reviews as protective factors against cyberbullying victimization (Kowalski et al., 2019; Zych et al., 2019).

Regarding group differences, there is an emerging trend in terms of gender differences and there is largely mixed evidence when considering disparities by race and ethnicity. With respect to gender differences, girls appear to be at greater risk (Kann et al., 2018; Kowalski et al., 2019), and this will be addressed in more detail in the next section. Explorations into ethnic and racial differences in cyber-victimization have yielded mixed-results (Kowalski et al., 2019), though some evidence suggests that whites experience cybervictimization at higher rates compared to their black and Hispanic counterparts (Kann et al., 2018). Additionally, there is some evidence that Arab-Americans may be distinctly targeted in cyberbullying (Kowalski et al., 2019). Other forms of bias-based bullying are supported in the literature in that the LGBTQI community, those with disabilities, and individuals with elevated weight status have also been identified as at-risk (Kowalski et al., 2019). The Youth Behavior Risk Surveillance from the Centers for Disease Control found that LGBTQI youth reported cyber-victimization rates over twice as high as those reported by their heterosexual counterparts (27.1% and 13.3% respectively) (Kann et al., 2018). Absent from the literature is any mention of religious minorities.

Factors predictive of cyberbullying perpetration have also been documented in the literature. For cyberbullying perpetration, individual-level risk factors include: low self-esteem, empathy, self-control, and high levels of impulsivity, moral disengagement, anxiety, aggression, and traditional bullying victimization (Kowalski et al., 2019). Alternatively, high self-esteem, social competence, and emotional management have been identified as protective factors (Kowalski et al., 2019; Zych et al., 2019). High technology use has been identified as an individual-level risk factor for cyberbullying perpetration (Kowalski et al., 2019), and low use has been identified as a protective factor (Zych et al., 2019). With regard to the family realm, a positive parent relationship and home environment have been found to be protective (Kowalski et al., 2019; Zych et al., 2019), and parental supervision of technology has also been identified as a protective factor (Zych et al., 2019). Regarding the peer domain, positive peer interactions as well as peer support have been identified as protective factors (Kowalski et al., 2019; Zych et al., 2019). Conversely, peer rejection, lack of prosocial peers and peer norms supporting bullying have been identified as risks (Kowalski et al., 2019). School and community factors including a positive school climate and satisfaction with school have found to be protective against cyberbullying perpetration (Kowalski et al., 2019; Zych et al., 2019). With regard to group differences, the evidence on gender differences and race and ethnic disparities in cyberbullying is mixed (Kowalski et al., 2019).

There is substantial overlap in the risk and protective factors for both victims and perpetrators of cyberbullying. This is likely due to the most vulnerable group of youth who are both targets of bullying and perpetrators of it—bully-victims. More work is necessary to better understand this vulnerable group in order to design more effective programming to address their needs.

5.1. Gender differences

Mixed evidence exists about gender differences in cyberbullying though a preponderance of evidence points to females being at greater risk of involvement (Kann et al., 2018; Kowalski et al., 2019). In point of fact, the most current results of the Youth Behavior Risk Surveillance from the Centers for Disease Control indicate that females reported nearly twice as high cybervictimization as males (19.7% and 9.9% respectively) (Kann et al., 2018). Other studies suggest no gender differences (see Wong et al., 2018 for a brief review).

Such inconsistencies in the literature point to the likelihood that that there are more nuanced differences in the ways that males and females relate online and how each group interacts in cyberbullying situations. According to Wong et al. (2018), males in their study were more likely to engage in cyberbullying perpetration if they had been previously victimized, whereas for females, they were more motivated by the disinhibition effect. These gender differences imply that males and females engage in cyberaggression for different reasons in cyberspace: males possibly using it to seek revenge while females may feel...
emboldened in situations where their accountability is diminished online. The motivation for males to seek revenge for prior cyberbullying concurs with the overrepresentation of males in the cyberbully-victim category found in other studies (Fahy et al., 2016).

Beyond gender differences in motivations for cyberbullying perpetration, the literature has also begun to explore gender differences in the topics that individuals who perpetrate cyberbullying choose to use. For example, one study found that in a sample of undergraduates, females were more likely to be targeted with topics about sexual activity (e.g., nude photos, etc.), whereas men were more frequently cyberbullied about their skills/talents (e.g., intelligence) and sexual orientation (Brody & Vangelisti, 2017). Again, these findings not only point to the need for further work exploring gender differences but also should catalyze more in-depth examination of bias-based forms of cyberbullying.

6. Outcomes

Vaillancourt et al. (2017) provide an excellent overview of the unique effects of cyberbullying—over and above traditional bullying—on mental wellbeing. The plethora of research reviewed by them indicate that after controlling for traditional bullying, cyberbullying is associated with: anxiety, depression, suicidal ideation and suicide attempts, somatic complaints and compromised physical health, symptoms of post-traumatic stress disorder (PTSD), and academic difficulties. Regarding intensity of psychopathology, the authors state “a dose-response effect is commonly found between being cyberbullied and the severity of its consequences—youth who are bullied the most are the ones who suffer the most” (Vaillancourt et al., 2017, p. 370).

Similar conclusions have been drawn by others about the ill-effects of cyberbullying. In a longitudinal study which controlled for baseline levels of distress, cyberbullying was associated with higher mental distress, depression, suicidal ideation and suicide attempts, somatic complaints and compromised physical health, symptoms of post-traumatic stress disorder (PTSD), and academic difficulties. Regarding intensity of psychopathology, the authors state “a dose-response effect is commonly found between being cyberbullied and the severity of its consequences—youth who are bullied the most are the ones who suffer the most” (Vaillancourt et al., 2017, p. 370).

7. Prevention and intervention

As a discipline, developmental psychopathology requires specific criteria in the design of effective prevention and intervention programming, including (1) theory which provides a foundation from which all strategies are based on; (2) an emphasis on risk and protective factors that have been identified in the empirical literature; (3) prominence of the various contexts that impact an individual (i.e., home, school, etc.) in program design; and (4) empirical evaluation of the program’s effectiveness (Hinshaw, 2013). Accordingly, there are several limitations in the programming literature on the issue, namely (1) programs have either been designed as extensions of traditional bullying programs, or a-theoretically (Tanrikulu, 2018); (2) much of the literature focuses on examining factors influencing involvement in cyberbullying on a one-context-at-a-time basis (i.e., parental monitoring or school-based remedies), but seldom together in a holistic framework; and (3) program evaluation has been limited due to variations in “duration, theory, sampling, design, and measurement tools” (Tanrikulu, 2018, p. 84).

Prior to addressing the various contexts for which programming has been developed, it is important to discuss the findings of the only published cyberbullying program reviews to date (1) Van Cleemput et al. (2014) reviewed eight programs across nine countries and conducted a meta-analysis; (2) Tanrikulu (2018) reviewed seventeen programs across the same nine countries; and (3) Gaffney, Farrington, Espelage, and Ttofi (2019) included twenty-four publications published from 2012 onward in their meta-analysis on cyberbullying program effectiveness. All three analyses examined studies based on school-aged samples and all concluded that programs demonstrated only modest effects. The meta-analysis conducted by Van Cleemput et al. (2014) found an average effect size for reducing victimization g = 0.135 (n = 9453, k = 6, 95% CI 0.079; 0.190, p < .001), while for perpetration it was g = 0.065 (n = 6373, k = 6, 95% CI 0.019; 0.112, p < .01). Alternatively, Gaffney et al. (2019) found overall reductions in cyberbullying victimization to range between 14 and 15% and for cyberbullying perpetration to range from 9 to 15%. These rates are modest and are commensurate with the effects gleaned in traditional bullying programs (Gaffney et al., 2019; Van Cleemput et al., 2014).

Regarding program strategies at school, Gaffney et al. (2019) did not explicitly analyze this and Van Cleemput et al. (2014) concluded that most programs did not adopt a whole school approach, but rather focused on modules implemented to address cyberbullying added on to their traditional anti-bullying programs. This is unfortunate given the large body of literature noting the centrality of a whole school approach in bullying prevention (see Ansary, Elias, Greene, & Green, 2015a, 2015b for a review).

Given the dearth of holistic programs addressing cyberbullying, I examine program strategies that are sensitive to risk and protective factors and that are also context-specific. This perspective aligns with Swearer and Hylen’s (2015) social-ecological diathesis-stress model, which conceptualizes the individual who bullies in a dynamic interaction with his/her home, school, peer-network, and neighborhood/community. Thus, the following section will examine evidence-based program strategies for parents, schools, bystanders, and social media platforms separately.

7.1. Parents

Positive parenting dimensions have been found to be a protective factor for both cybervictimization and cyberbullying perpetration (Kowalski et al., 2019). Parental supervision of technology is also a protective factor in cyberbullying perpetration (Zych et al., 2019). This is no surprise as parents are recognized as an important target audience in traditional bullying prevention (Ansary et al., 2015a; Ansary et al., 2015b), and they may even be more critical agents in cyberbullying prevention and intervention.

With regard to monitoring of technology, according to Pew Research Center (Anderson, 2016), parents may be relatively hands-on in monitoring their children’s technology use. In point of fact, 60% of parents say they check their teens’ social media profiles, and 48% have ever looked through their teens’ phone calls or texts (Anderson, 2016). And while many parents recognize this important role, they report lacking the technological knowledge to comprehensively monitor (Kessel Schneider, Smith, & O’Donnell, 2013). Although online tip sheets are an important source of information for parents, Espelage and Hong (2017) caution that these may not be vetted and accordingly recommend that parents seek guidance from government agencies or advocacy organizations that are evidence-based.

Guidance for parents should include information on prevention (e.g., teaching children digital citizenship) and intervention when cyberbullying happens (e.g., block users who post harmful messages). Regarding prevention, parents should instruct their children about safe ICT use, such as (1) not sharing usernames or passwords; (2) not providing personal information in profiles, chat rooms, and other fora; (3) not responding to threatening messages and to notify an adult immediately; and (4) shutting technology off if a threatening message is
received (National Crime Prevention Council, n.d.). Nurturing responsible use of technology also entails instructing youth (1) about refraining from sending personal or inappropriate photos of oneself; (2) that a post leaves a permanent footprint that cannot be taken back (National Crime Prevention Council, n.d.); (3) to tell an adult without fear of losing access to their technology; and (4) that consequences will be firmly enforced for engaging in cyberbullying perpetration (see Hinduja & Patchin, 2013). With respect to intervention when cyberbullying occurs, evidence suggests that engaging the child who bullies in further online communication about the incident exacerbates the problem (Perren et al., 2012), and accordingly parents should immediately block the potential cyberbully from any further communication. Reporting the attack to the appropriate social media outlet is also a critical step. Although parents may be challenged to effectively monitor children’s ICT use, they can certainly make a difference.

7.2. Educators and schools

School climate and satisfaction with school are protective factors for both targets of cyberbullying and individuals who perpetrate cyberbullying (Kowalski et al., 2019; Zych et al., 2019). In prior research, cyberbullying was characterized as occurring outside of school with negative interactions continuing into the next school day (see Cassidy, Faucher, & Jackson, 2013). More recent trends indicate that the dichotomy between technology use at school versus at home is no longer an important distinction. Adolescents often have access to computers or tablets while at school, and though many schools ban cell phone use, the reality is that most youth use them during the school day. In a similar vein, schools also provide the context within which peers interact socially and since most targets of cyberbullying know the perpetrator (Whittaker & Kowalski, 2015), schools must play an important role in prevention and intervention. Cumulatively, these risks underscore the need for effective and explicit school-based cyberbullying programming. As will be discussed later, laws in all fifty states in the U.S. hold schools accountable for preventing, intervening, as well as investigating and reporting cyberbullying (U.S. Department of Health and Human Services, 2018).

Fostering a positive school climate is crucial in the prevention of traditional bullying and cyberbullying (Ansary et al., 2015a; Ansary et al., 2015b; Espelage & Hong, 2017). Moreover, Espelage and Hong (2017) note that with regard to cyberbullying, schools should (a) have clear proactive policies, procedures, and practices about internet use and cyberbullying; (b) actively promote awareness of social-emotional skills among faculty, staff, and students; (c) promote a positive school environment; and (d) nurture school-family connections. While these are no different than essential elements of effective school-based anti-bullying programs, an explicit emphasis on bullying in cyberspaces is critical. Some evidence suggests that cyberbullying is not always explicitly mentioned in schools’ anti-bullying policies (Kessel Schneider et al., 2013). This is unfortunate in light of research evidence suggesting that youth who report having clear rules about cyberbullying from school and parents are significantly less likely to report involvement in online bullying (Hinduja & Patchin, 2013).

Other areas where schools can work towards preventing cyberbullying, is to directly tackle the issue through the school’s curriculum in a developmentally appropriate fashion. The evidence is clear that social emotional character development (SECD) is one of the central columns that effective anti-bullying programs are built on (Ansary et al., 2015a; Ansary et al., 2015b). The cyberbullying prevention literature is rife with synonyms for socially responsible behavior (e.g., prosocial behavior, kindness, etc.) though many researchers do not specifically refer to these as social-emotional skills. Just as it is in traditional bullying prevention, SECD should play a prominent role in cyberbullying prevention. Another critical element in addressing cyberbullying in schools is professional development: Teachers need to be trained to identify, respond, and report incidents to the necessary channels the school has in place to address cyberbullying (Ansary et al., 2015a; Ansary et al., 2015b; Espelage & Hong, 2017).

7.3. Peers and bystanders

For both cyberbullying targets and perpetrators, positive peer interactions and peer support are protective factors (Kowalski et al., 2019; Zych et al., 2019). Conversely, peer rejection, lack of prosocial peers and peer norms supporting bullying are risks for cyberbullying perpetration (Kowalski et al., 2019). Allison and Bussey (2016) found that one of the strongest predictors of cyberbullying bystander intervention is whether or not the target of the bullying is a friend.

Bystanders play a key role in defusing or escalating incidents in both traditional and cyberbullying domains (Allison & Bussey, 2016). According to Lenhart et al. (2011) 88% of U.S. teens have witnessed cyberbullying and of these, 91% reported that they did nothing about it. Lack of bystander intervention can be explained by several factors, namely (a) whether posts occur on large platforms where youth feel that others will likely intervene (diffusion of responsibility); (b) worry over what others will say; and (c) because of the asynchronous nature of cyber-interactions, youth may feel that it is too late to act (Allison & Bussey, 2016). According to Allison and Bussey (2016) these characteristics of bystander intervention have been replicated cross-culturally.

7.4. Social media

Social media companies must walk the fine line between regulating free speech (i.e., policing and removing content that may be harmful or offensive), and protecting the rights of users (Milosevic, 2016). Consequently, these companies often “…downplay their own responsibility for the extent to which technologies may facilitate such behavior…” and “they see users as better positioned to understand the context behind their own conflicts” (p. 5175). Accordingly, many social media companies advocate for social reporting or community moderation to address cyberbullying because it is more efficient for the company though not necessarily in the best interest of users (Milosevic, 2016).

Larger social media companies tend to have a more comprehensive definition of cyberbullying as well as more sophisticated policies and procedures in place to help support users compared to younger companies (Milosevic, 2016). Most social media platforms have mechanisms to prevent and intervene in cyberbullying such as: reporting, blocking, filtering software, as well as human and automated detection systems. Automatic detection through feature engineering (Rosa et al., 2019) examines various characteristics of posts (e.g., language, emotions, etc.) to identify instances of cyberbullying. In a review of automatic cyberbullying detection studies, Rosa et al. (2019) conclude that current detection systems do not distinguish between cyberaggression and cyberbullying: Those researchers recommend annotator training on the proper definition and overall concept of cyberbullying (Rosa et al., 2019). Further, automatic detection systems may be less efficient since human moderators can understand nuances in language such as irony or context-specific aggression (Milosevic, 2016).

Beyond explicit guidance on intervention, social media companies should do more to prevent cyberbullying. Some prevention efforts employed by social media platforms include (1) messaging about appropriate online behavior and a focus on positive instead of negative interactions (Barlett, DeWitt, Maronna, & Johnson, 2018; Kessel Schneider et al., 2013); (2) notifications and delays that are designed to promote self-reflection and prosocial behaviors (Rosa et al., 2019), such as proactive screening, which can identify potentially harmful posts and prompt the user with messages such as “Are you sure you want to post this?” or “Say something kind” (see Milosevic, 2016, p. 5172); (3) require users’ to reveal their identities since sites that do so report lower levels of cyberbullying than those that do not (Barlett et al., 2018); and (4) require users to authenticate their account and emails regularly to
prevent the use of fake accounts (Barlett et al., 2018). Furthermore, social media platforms should encourage bystanders to intervene (Barlett et al., 2018) even if by the more commonly seen indirect methods of intervention (e.g., rating a post unfavorably or reporting the perpetrator) as opposed to direct intervention (explicit correspondence about the incident) (Barlett et al., 2018).

7.5. Health care providers

Since reporting of cyberbullying involvement is extremely low (Cassidy et al., 2013), medical doctors and mental health practitioners working with adolescents may play important roles in detecting it. These health professionals can ask questions about cyberbullying (either directly or by survey) at intake and encourage youth to speak with parents about limiting technology (Espelage & Hong, 2017). For mental health practitioners, the link between cybervictimization and myriad forms of long-term psychopathology are well documented (Vaillancourt et al., 2017). Furthermore, the important role of mental health practitioners is underscored by evidence (that requires replication) suggesting that even incidents that happened in the past are associated with present-day dysfunction (Rosenthal et al., 2016).

7.6. Law

Although all fifty states in the U.S. have laws addressing cyberbullying, there is considerable variability in their protections and the U.S. Department of Education has provided federal guidance on the issue since 2010, in an effort to promulgate a basic standard for protections (U.S. Department of Health and Human Services, 2018). Given variability across states, Hinduja and Patchin, (2015b) outline six recommendations for laws addressing effective anti-cyberbullying policies. These include (1) a specific definition of harassment, intimidation, and bullying with explicit mention of various technologies; (2) sanctions that increase in severity based on repetition; (3) clear policies for reporting; (4) clear policies on investigating; (5) explicit mention of activities occurring off-school grounds that constitute cyberbullying; and (6) policies and procedures for preventing cyberbullying. These are nearly identical to best-practices for school-based programming to address traditional bullying (Ansary et al., 2015a, 2015b). These laws hold educators and administrators responsible for effectively intervening, investigating, and reporting, as well as for the implementation of effective cyberbullying prevention programming.

8. Limitations and future directions

While it is encouraging to see an explosion in the empirical investigation of cyberbullying, significant limitations in the field persist and more scholarship is required. The most general limitations in the existing literature surround the difficulties of a definition, inconsistent ways of measuring cyberbullying, and limited theories holistically explaining the issue. While progress has occurred in terms of a definition, greater work is needed on the construction of reliable and valid measurement of cyberbullying that effectively discriminates it from cyber-aggression. Doing so will foment progress in terms of strengthening the internal validity of studies examining cyberbullying, as well as establish accurate prevalence rates.

Regarding theoretical models explaining cyberbullying from a psychological perspective, with the exception of Swearer and Hymel’s (2015) social-ecological diathesis-stress model, the existing models are too simplistic and do not adequately account for the existing risk and protective factors that have been empirically identified. Moreover, in light of recent evidence suggesting gender differences in cyberbullying perpetration (Kowalski et al., 2019; Wong et al., 2018), theoretical models will need to explicitly account for gender. Inclusion of variables assessing other minority identities (i.e., racial, ethnic, religious, sexual, etc.) is also necessary as these individuals are elevated risk of being targeted. Additionally, prior victimization is a critical variable that should be present in theoretical models of cyberbullying, given that it has been repeatedly identified as a risk factor (Kowalski et al., 2014, 2019; Waasdorp & Bradshaw, 2015; see also Wong et al., 2018). Such insights necessitate the refinement of existing models to account for these complexities and also point to the need for the creation of more complex models that comprehensively capture the problem. Progress in the development of holistic theoretical models that are tested among diverse samples (e.g., heterogeneity in age, race, ethnicity, sexual orientation, disability, etc.) and using various methodologies is needed to undergird progress in the scholarly and applied realms.

There are no prospective longitudinal studies published regarding risk and protective factors and thus the findings are mainly related to cross-sectional research (Zych et al., 2019). Furthermore, more elaborate research designs are needed to adequately capture the dynamic interactions between individual, familial, peer, school, and community levels in the exploration of risk and protective factors. For example, Savage and Tokunaga (2017) concluded that cyberbullying perpetration was explained by a complex relationship of social skills, internet self-efficacy, and verbal aggressiveness. As such, prospective longitudinal analyses that examine these dynamic interactions is necessary and path analysis, structural equation modeling, and person-based analysis will provide useful insights into the complexity of cyberbullying.

Study of group differences in the risks for cyberbullying victimization and perpetration has just begun. More work is required to further explain the mixed evidence about gender differences, which can only occur by exploring the differences in motivations for technology use, the salience of the disinhibition effect, coping with prior victimization, among other factors between males and females (Wong et al., 2018). Moreover, scant evidence on bias-based forms of cyberbullying exist (Kann et al., 2018; Kowalski et al., 2019) and these suggest groups of understudied populations that are particularly vulnerable. In spite of evidence regarding disproportionately higher rates of traditional bullying of Muslim, Jewish, and Sikh youth (Ansary, 2018), there are no peer-reviewed studies addressing cyberbullying of religious minorities. While it may not be the case that these youth are explicitly targeted with reference to their minority identity (e.g., Muslim youth being called a terrorist), they are likely to be, more broadly, at elevated risk for all forms of cyberbullying.

Evidence-based prevention and intervention efforts will benefit from work that addresses the existing limitations in the field. At this time, cyberbullying programs have limited or no theoretical basis, are often considered as an add-on module to traditional bullying programs, and have not been evaluated in meaningful ways to determine effectiveness (Tanrikulu, 2018; Van Cleemput et al., 2014). Strides are necessary to build-on the growing body of research pointing to specific risk and protective factors that are context-specific in order to design more effective programs. Furthermore, there should be an urgent call for policy makers to develop restrictions on social media applications that are advertised to younger users that will ensure better prevention and intervention of cyberbullying.

9. Conclusion

If the next ten years of research mirrors the exponential growth in the cyberbullying literature that we have seen in the past ten years, the field should be equipped with well-designed effective prevention and intervention programming. Moreover, progress must address the empirical evaluation and tailoring of prevention and intervention programs to address the needs of our most vulnerable youth, namely, racial/ethnic and religious minorities, LGBTQI individuals, and persons with varying abilities. Empirically informed prevention strategies that address the gamut of an adolescent’s life will eventually offer the protection that every child deserves.


