Review

Cyberbullying or Cyber Aggression?: A Review of Existing Definitions of Cyber-Based Peer-to-Peer Aggression

Lucie Corcoran 1,*, Conor Mc Guckin 2 and Garry Prentice 1

1 School of Arts, Dublin Business School, Dublin 2, Ireland; E-Mail: Garry.Prentice@dbs.ie
2 School of Education, Trinity College Dublin, Dublin 2, Ireland; E-Mail: conor.mcguckin@tcd.ie

* Author to whom correspondence should be addressed; E-Mail: lucie.corcoran@dbs.ie; Tel.: +353-(0)1-4178769.

Academic Editor: Gregor Wolbring

Received: 11 January 2015 / Accepted: 18 March 2015 / Published: 27 March 2015

Abstract: Due to the ongoing debate regarding the definitions and measurement of cyberbullying, the present article critically appraises the existing literature and offers direction regarding the question of how best to conceptualise peer-to-peer abuse in a cyber context. Variations across definitions are problematic as it has been argued that inconsistencies with regard to definitions result in researchers examining different phenomena, whilst the absence of an agreed conceptualisation of the behaviour(s) involved hinders the development of reliable and valid measures. Existing definitions of cyberbullying often incorporate the criteria of traditional bullying such as intent to harm, repetition, and imbalance of power. However, due to the unique nature of cyber-based communication, it can be difficult to identify such criteria in relation to cyber-based abuse. Thus, for these reasons cyberbullying may not be the most appropriate term. Rather than attempting to “shoe-horn” this abusive behaviour into the preconceived conceptual framework that provides an understanding of traditional bullying, it is timely to take an alternative approach. We argue that it is now time to turn our attention to the broader issue of cyber aggression, rather than persist with the narrow focus that is cyberbullying.

Keywords: cyber aggression; cyberbullying; cyber victim; cyber victimization; definitions; bullying
1. Introduction

This paper asserts a position to progress the conceptualisation and definition of cyber-based aggressive behaviours, generally classed under the term cyberbullying. A review of definitional approaches to both traditional bullying and cyberbullying is provided so as to highlight the similarities but, also, crucially, the differences between the “real world” and cyber settings. In this way, it becomes evident that the traditional bullying definitional criteria do not provide an easy match to the cyber context. In addition, different theoretical perspectives on the conceptualisation of cyberbullying further emphasise the need to consider different perspectives on cyber-based aggression [1]. Whilst it is acknowledged that important contributions have been made to progressing the definition of cyberbullying [2], recent findings [3] have highlighted the need to adopt a different approach. Ultimately, we will present a synopsis of the problematic nature of the label “cyberbullying” and current definitions, and we will present a way forward for the research community. In order to gain insight regarding the rationale for cyberbullying definitions, it is important to first review the defining components of traditional bullying.

2. Defining Bullying for a “Real World” Setting

Presently there is an ongoing debate regarding the existence of cyberbullying, the extent of the problem, and the threat that cyber-based abuse carries (see Olweus and Smith for a scholarly engagement [4,5]). Central to this debate is how we delineate the behaviours and actions that are commonly labelled as “cyberbullying”; that is, how we identify the parameters of the phenomenon, what we recognise as the inclusion and exclusion criteria as part of the definitional stance, and importantly, how we conclude that cyberbullying is in fact the correct term for the behaviour that we are exploring.

Within the realm of “traditional bullying” research, sometimes referred to as face-to-face (f2f) bullying [6], there is wide consensus regarding the defining criteria, namely (a) intent to cause harm [7,8], (b) repetition of the behaviour over time [7,9,10], and (c) an imbalance of power between the victim(s) and bully(ies) [7,8,10]. However, with the emergence of cyberbullying, the central question for researchers and practitioners relates to the extent to which the same criteria could be “plugged into” a definition of cyberbullying.

Definitions of traditional bullying have reflected the static nature of the “real world” setting, which is characterised by boundaries of time and geography (e.g., school, home). However, abuse of peers is no longer confined to the school setting, nor is it restricted to the typical daily routines of human interaction; characteristics that bind instances of traditional bullying. Indeed, the capacity to use electronic devices and media to attack someone in almost any location, and at any time, is a distinctive feature of cyber-based abuse [11]. Moreover, there is the potential for abusive or humiliating content to be disseminated to an audience of unknown size and location [12]. This allows for the notion of “repetition” in operational definitions to take a different form in the cyber world, as abusive behaviour need not be repeated on the part of the aggressor [13] in order for the target to experience repeated victimization, as the bystanders take a central role in cyber-based abuse through their viewing, “sharing”, and “liking” of humiliating content, such as comments (e.g., tweets, texts), pictures, and
videos. Moreover, the element of “power”, another central aspect of operational definitions of traditional bullying, is somewhat more difficult to determine in a cyber context. For example, power could be characterised by the ability to remain anonymous in cyberspace, or the ability to capitalise on superior technological skills [13]. It could also be characterised by the immediacy of the dissemination and the capacity to humiliate on a grand scale [14]. Moreover, the challenges faced by researchers do not end here—the very nature of cyberspace as an evolving entity presents a formidable challenge.

3. Defining Cyberbullying in an Ever Changing Cyber Environment

The term “cyberbullying” was initially a convenient label for abusive behaviour perpetrated through the use of mobile telephones and computers with Internet access. However, in less than ten years, and in homage to Moore’s Law [15], the exponential development of the consumer technology market has witnessed the migration from immobile desktop computers with slow, dial-up Internet connections, to tablets and pocket size Smartphones, which allow for recording and publishing of material online in mere seconds. Thus, unlike their Cro Magnon ancestors who “…may have had to settle for daubing unflattering pictures of their peers on cave walls…” [16] (p. 679), the tools of modernity enable the children and adolescents of today to paint unflattering pictures in a more remote, covert, and insidious manner.

Thus, attempting to operationally define cyberbullying in a world which is in constant flux, could be likened to asking time to stand still. The evolving features of the available technology only intensify the unique nature of the communication. Indeed, whilst we debate and dialogue about the defining characteristics of cyberbullying, we must remain cognisant that by the time we reach some form of consensus, children and adolescents will, in all likelihood, be using technology and social communication tools that do not yet exist. What we as researchers and practitioners refer to as bully/victim problems must be understood in the context of this post-modern world. Perhaps the most important question that requires attention is: how do we operationalise and define these behaviours and intentions for the children of the 21st Century?

4. Practical Implications of Cyberbullying Definitions

This issue becomes particularly important at a practical level. The importance is evident in relation to the application of knowledge to prevention and intervention efforts (e.g., CyberTraining: http://www.cybertraining-project.org; CyberTraining-4-Parents: http://cybertraining4parents.org). Past research has provided a wealth of evidence that there is an overlap between traditional bullying and cyberbullying (e.g., Olweus, 2012 [4]), and therefore the literature pertaining to traditional bullying intervention and prevention efforts can inform our efforts to counter cyberbullying. Therefore, it would be important to establish whether the same degree of overlap remains if the focus were to shift to cyber aggression more broadly rather than cyberbullying specifically. In other words, if the characteristics of cyber-based aggression are in fact different to those of traditional bullying, can we still make clear links between the two forms of aggression when designing prevention and intervention initiatives for cyberspace? Overall, a better approach to defining and measuring cyber-based aggressive behaviour would support better intervention and prevention efforts intended to reduce the incidence of such harmful behaviours. Evidence informed interventions and preventative mechanisms
Although the impact of cyber-based abuse can be best understood in terms of “coping”—whether at the systemic, familial, or personal level [17]. That is, coping can be viewed on distinct levels, including policy implementation (e.g., corporate social responsibility activities of organizations involved in hardware/software components of the industry) and legislation, and by extension quasi-legislative instruments such as the EU Convention on the Rights of the Child. At a national level, responses and policies become important vessels for disseminating guidance and support for the population (see O’Moore et al. [18] for an overview of the work by the COST (European Cooperation in Science and Technology) IS0801 network: https://sites.google.com/site/costis0801). For instance, the Irish Department of Education and Skills [19] have updated their Anti-Bullying Procedures for Primary and Post-Primary Schools, and it would be hoped that this iterative development reflects the work regarding definitions of the aforementioned groups. It is important that both the conceptualisation and operationalisation of cyberbullying by researchers and practitioners is appropriate as we develop our understanding of the ways in which individuals cope effectively (see Mc Guckin and colleagues [20] for an overview of the literature pertaining to coping as part of the work by the COST (European Cooperation in Science and Technology) IS0801 network). Despite the limitations and challenges to impose traditional bullying criteria in a cyber setting, efforts to define cyberbullying to date have largely centred on this approach.

Finally, the way in which we label and define problematic cyber-based behaviour has real implications for protecting mental health. Due to the fact that there is potential for wide public access to online content, a single cyberbullying incident could have a serious and lasting harmful effect on the victimised person. Therefore, refining the definition and conceptualisation of cyber-based aggression could have serious implications for protecting mental health, as no longer would a young person have to endure multiple episodes of victimization before the behaviour could be recognised as cyberbullying. By removing the component of repetition from the conceptualisation of cyber aggression, we would be recognising the potential for one single act to cause psychological harm to a targeted person.

5. How We Have Defined Cyberbullying Thus Far?

Offering one of the earliest definitions, Belsey [21] defined cyberbullying as “…the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others”. Applying the existing criteria regarding traditional bullying, and alluding to the potential power imbalance, Smith and colleagues [22] later defined 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). Perhaps the most comprehensive and useful early definition was offered by Tokunaga [23], who built upon existing definitions to define cyberbullying as “…any behavior performed through electronic or digital media by individuals or groups that repeatedly communicates...
hostile or aggressive messages intended to inflict harm or discomfort on others” (p. 278). However, considering the unique aspects of cyberspace, one must question how appropriate the label of cyberbullying and, by extension, existing definitions, really are.

Langos [14] argued that the core elements of traditional bullying (i.e., repetition, power imbalance, intention, and aggression) also underpin cyberbullying, but insisted that we must distinguish between direct (private communications such as a text message) and indirect (communication in a public domain, such as a social networking site) forms of cyberbullying. Langos [14] argued that the repetitious nature of the behaviour is more evident in direct cyberbullying where repeated actions on the part of the cyberbully are necessary to characterise repetition. It was suggested that repeated actions on the part of the cyberbully may also indirectly expose the criterion of intent to cause harm. As the intent may be more difficult to identify in cases of indirect cyberbullying, Langos [14] recommended that intentionality is determined based upon how a reasonable person would assess the aggressor’s conduct. However, taking an alternative perspective by focusing on cyber aggression in a broader sense, Grigg [1] has made an important contribution to the debate.

6. An Alternative Approach—What about Cyber Aggression?

Grigg [1] took a rather different approach, arguing that the term cyberbullying raises a number of difficulties. With respect to the element of power, Grigg [1] argued there is little evidence to suggest that cyberbullies have superior technological skills, and additionally indicates that there is a lack of clarity regarding whether responsibility lies with the cyberbully or the bystanders when repetition takes the form of repeated views of humiliating content. Considering the broad range of negative acts that can occur in cyberspace, Grigg [1] defined “cyber aggression” as “…intentional harm delivered by the use of electronic means to a person or a group of people irrespective of their age, who perceive(s) such acts as offensive, derogatory, harmful, or unwanted” (p. 152). This argument, that there is a need to look at aggression more broadly, is one that has received little consideration since its publication, but must be given regard in light of the difficulties in achieving a satisfactory cyberbullying definition.

Pyżalski [24] proposes a typology of electronic aggression based on the identity of the targeted individual(s), arguing that the framing of cyberbullying within the school bullying conceptualisation involves the assumption that all aggressive behaviours occur within the peer group. Therefore, Pyżalski’s typology [24] includes both peer-directed cyber aggression and electronic aggression targeting celebrities, groups, vulnerable individuals, school staff, and random victims. In a large scale study of Polish adolescents, Pyżalski [24] measured electronic aggression (characterised by intention as a traditional bullying criterion), and cyberbullying (also including the characteristics of repetition and power imbalance). In this way, similar to Grigg’s approach, an important distinction was made between the traditional bullying criteria and cyber aggression more broadly. However, an important voice which also deserves attention, is that of our research population—children and adolescents. Pyżalski’s typology [24] of electronic aggression was in fact based on qualitative interviews with teachers and students. This leads us to a vital consideration—if we create a cyberbullying concept which does not fit with the youth perspective, then what use is it?
7. How to Approach This Issue—Bottom-Up or Top-Down?

If the academic literature asserts that the negative experiences of children in cyberspace can be conceptualised as cyberbullying with agreed definitional parameters, the question arises, does this hold true for what children and young people think? In essence, are we applying a top-down approach to the area whereby experts deliver the terminology and definition as dogma without any reflection upon the voice of children, or their ability to co-construct meaning with researchers [25]? As we know from the literature regarding traditional bullying, when asked and involved in research which takes a bottom-up approach, children and young people may report a different perspective [26]. Menesini [27] provides an overview of recent research which has consulted student voice in an attempt to counter the “top-down” approach to definitions and labelling, and reports that the criteria for traditional bullying are also relevant for cyberbullying. Further, Menesini [27] states that whilst the additional aspects of publicity and anonymity can be useful in relation to identifying the severity of the cyber-based abuse, the relationship between the aggressor and victim, as well as the response from the victim, these aspects are not necessary for recognising behaviour as cyberbullying.

8. Involving Student Voice

An important contribution in this area was that by Menesini and colleagues as part of an international collaborative initiative (the COST [European Cooperation in Science and Technology] IS0801 network). In order to consider and advance the definition of cyberbullying, Menesini and colleagues [2] collected qualitative data from young people via focus groups across Italy, Spain, Germany, Sweden, and Estonia, as well as quantitative research via a questionnaire with the same countries and France in addition. Acknowledging the debate as to whether the criteria for defining traditional bullying are relevant for cyberbullying, the research group also sought to ascertain if the cyber-specific components of publicity and anonymity were key criteria. The focus groups revealed that intent, effect on the victim (as part of a power imbalance), and repetition (can indicate the intent and severity of the victimization) were all recognised as criteria for defining cyberbullying. Questionnaire results revealed that the power imbalance (in the form of consequences for the victim and inability to defend themselves) and intent were perceived as key criteria, whilst repetition was not regarded as a key characteristic.

Based on the overall analysis, Menesini and colleagues [2] drew conclusions regarding the appropriate defining components. One of the focus groups revealed that intentionality was less important for defining cyberbullying than the effect on the victim, as unintentionally harmful acts can have a detrimental effect on the victim. Therefore, Menesini and colleagues [2] concluded that intent should be considered a criterion for cyberbullying, although it remains unclear whether the perpetrator or victim perspective is more important. With respect to power imbalance, Menesini and colleagues [2] concluded that although it is difficult to define precisely how someone is less powerful in cyberspace compared with another person, the power imbalance can take different forms and makes the victim feel less powerful and causes difficulty in relation to defending him/herself. Power imbalance was considered by the research team to be a more important criterion than intentionality. Although repetition did not emerge as a key criterion from the questionnaire results, and despite their
acknowledgement of the complex nature of repetition in a cyber context, Menesini and colleagues [2] suggest that it is a relevant criterion for defining cyberbullying as it distinguishes a joke from cyberbullying and it also highlights the distinction between cyberbullying and cyber aggression (as cyber aggression does not require repetition). Additionally, anonymity and publicity were considered to be significant factors but not defining characteristics of cyberbullying. Overall Menesini and colleagues [2] argued for the inclusion of intentionality and power imbalance to be included as key defining criteria of cyberbullying, whilst repetition received a lower level of agreement as a key criterion. The important research conducted by Menesini and colleagues [2] does much to progress the development of an agreed-upon definition of cyberbullying. However, it also highlights the complex nature of defining cyberbullying and reveals differing perspectives—even among students.

In addition, Vandebosch and Van Cleemput [28] collected data from 53 focus groups involving students aged from 10 to 18 years, with results supportive of the traditional bullying frame. Consistent with traditional bullying definitional criteria, “true” cyberbullying was found to be characterised by intention to cause hurt and perception of the behaviour as hurtful (by the victim), repetition of negative offline or online behaviours, and a power imbalance (based on “real-life” factors such as physical strength and/or on ICT-related criteria such as anonymity). With respect to repetition, just one online negative act in combination with traditional bullying was considered to constitute cyberbullying. Still, in light of the varying responses found by Menesini and colleagues [2] and also considering the challenges of traditional bullying criteria already outlined in this paper, is it in fact time for a fresh approach?

9. Time for a Fresh Approach—Evidence from Irish Research

Corcoran and Mc Guckin [3] provide evidence that the ways in which we label and measure cyber-based abuse can lead to marked differences in the reporting of victimization and perpetration of such behaviours. Using a survey approach, based on that designed by Swiss researchers [29], Corcoran and Mc Guckin [3] measured involvement in cyber aggression and cyberbullying among a sample of 2474 Irish second-level students aged between 12 and 19 years. Cyber aggression was measured using two nine-item scales (victimization and perpetration). With respect to cyber aggression, no definition was offered, but respondents were asked about the frequency of their experiences of specific aggressive behaviours in a cyber setting during the previous three months. By contrast, involvement in cyberbullying was measured by providing respondents with a definition of cyberbullying before presenting one item pertaining to perpetration of cyberbullying and one item pertaining to victimization by cyberbullying. Although both approaches were measuring the concept recognised in the academic literature as cyberbullying, the scale approach did not include a definition involving the traditional bullying criteria. Results revealed that, with a frequency of about once a month or more often, about once a week, or (almost) daily, 10.83% of respondents (n = 267) reported involvement as a victim of cyber aggression and 5.15% (n = 126) reported perpetration of cyber aggression. By contrast, just 2.24% of respondents (n = 55) indicated victimization by cyberbullying and 1.12% (n = 24) reported perpetration of cyberbullying. This provides some support for Olweus’ assertion that cyberbullying is a low prevalence phenomenon [4]. As Tokunaga [23] suggests, and repeatedly emphasised by Mc Guckin [17] regarding traditional bullying, the inconsistencies across the various
operational definitions (e.g., time reference periods for events to have happened) have resulted in researchers exploring different phenomena whilst using the same label (i.e., cyberbullying). Furthermore, where one researcher might insist on repetition for an experience to be considered cyberbullying, another will accept just one incident as cyberbullying. Findings by Corcoran and McGuckin [3] constitute an important signpost for researchers—highlighting the need to look at definitional and conceptual issues with “fresh eyes” and to be open to the possibility of an alternative approach. In other words, it is time to reframe the problem, rather than persisting with trying to “fit a round peg in a square hole”.

10. Why We Need to Reframe the Issue of Cyber-Based Abuse

In sum, a number of factors lead to the conclusion that the term cyber aggression may be a more appropriate term and concept than cyberbullying. First, cyberbullying implies a behaviour that is the cyber-based equivalent of traditional bullying, which in turn entails specific criteria (i.e., repetition, power imbalance, and intent to cause harm). However, the contextual features of cyberspace mean that such criteria are not easily applied. Secondly, despite research exploring young people’s perceptions of cyberbullying [2,28,30], there has been some difficulty in reaching a clear consensus regarding the defining aspects of cyberbullying. Thirdly, bullying is a form of social aggression [31] and thus cyberbullying would exclude incidents in which the aggressor(s) and victim(s) are strangers (e.g., happy slapping which would include acts such as using a camera phone to film a physical assault on a victim for the purpose of sharing it), which has implications in that education intended to prevent and counter cyberbullying would have a rather narrow scope. Surely it is more important to address all forms of aggression. Fourth, the findings of Corcoran and McGuckin [3] highlight the incompatibility between the academic understanding of cyberbullying and the student perception. Although this may highlight a need to educate students on the meaning of cyberbullying, perhaps the term cyber aggression would better serve our objectives. Indeed, the scale approach to assessing peer abuse in cyberspace revealed the incidence of behaviours which researchers and practitioners wish to better understand. Perhaps the term cyberbullying is in fact redundant and confusing. Fifth, the term cyberbullying may also carry a stigma which could account for the low incidence rate found by Corcoran and McGuckin [3]. This would further highlight the need for an alternative approach, and so a new focus on peer-directed cyber aggression is suggested.

11. Conclusion: A New Way Forward

Whilst Menesini [27] poses the question “How and to what extent might cyberbullying be underestimated if we neglect its specificity?” (p. 544), the present article poses the question, to what extent might we be underestimating the incidence and effects of cyber-based peer-to-peer abuse by constraining its conceptualisation and operationalisation with inappropriate criteria and labels? Perhaps the definition of aggression [32] which states that aggression is “…any behavior intended to harm another person that the target person wants to avoid” (p. 222) could be adapted for the purposes of cyber aggression. Therefore, also considering Langos’ suggestion regarding appraisal of intent [14] and Pyżalski’s inclusion of intent (but not repetition or power imbalance) when measuring electronic aggression [24], the following definition is proposed—“Cyber aggression refers to any behaviour
enacted through the use of information and communication technologies that is intended to harm another person(s) that the target person(s) wants to avoid. Intent to cause harm should be judged on the basis of how a reasonable person would assess intent.” In this way, the shackles of the traditional bullying framework can be removed, allowing a different path forward. Combined with Pyżalski’s approach of examining the identity of the targeted individual(s) [24], it is possible to distinguish between peer-directed cyber aggression and other-directed cyber aggression. There is already acknowledgement that cyber aggression is a behaviour which can be identified as, for example, online harassment or Internet harassment [2], and Grigg [1] has hinted at the “…vagueness, restrictiveness and ambiguity…” (p. 152) of the term cyberbullying and suggested that perhaps the focus needs to shift towards this broader approach—a suggestion worth considering as research, practice, and prevention work matures.

Author Contributions

Lucie Corcoran was the primary author of this paper and was responsible for the write up and revisions to the manuscript. Conor McGuckin was involved in the planning of the paper and also contributed feedback, and editing throughout the writing process. Garry Prentice contributed feedback and editing throughout the writing process.

Conflicts of Interest

The authors declare no conflict of interest.

References


© 2015 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).