



From risk factors to detection and intervention: a practical proposal for future work on cyberbullying

Andri Ioannou, Jeremy Blackburn, Gianluca Stringhini, Emiliano De Cristofaro, Nicolas Kourtellis & Michael Sirivianos

To cite this article: Andri Ioannou, Jeremy Blackburn, Gianluca Stringhini, Emiliano De Cristofaro, Nicolas Kourtellis & Michael Sirivianos (2018) From risk factors to detection and intervention: a practical proposal for future work on cyberbullying, Behaviour & Information Technology, 37:3, 258-266, DOI: [10.1080/0144929X.2018.1432688](https://doi.org/10.1080/0144929X.2018.1432688)

To link to this article: <https://doi.org/10.1080/0144929X.2018.1432688>



Published online: 08 Feb 2018.



Submit your article to this journal [↗](#)



Article views: 432



View Crossmark data [↗](#)



From risk factors to detection and intervention: a practical proposal for future work on cyberbullying

Andri Ioannou^a, Jeremy Blackburn^b, Gianluca Stringhini^c, Emiliano De Cristofaro^c, Nicolas Kourtellis^d and Michael Sirivianos^e

^aCyprus Interaction Lab, Department of Multimedia and Graphic Arts, Lemesos, Cyprus; ^bDepartment of Computer Science, University of Alabama, Birmingham, USA; ^cDepartment of Computer Science, University College London (UCL), London, UK; ^dTelefonica Research, Barcelona, Spain; ^eDepartment of Electrical Engineering, Computer Engineering and Informatics, Cyprus University of Technology, Lemesos, Cyprus

ABSTRACT

While there is an increasing flow of media stories reporting cases of cyberbullying, particularly within online social media, research efforts in the academic community are scattered over different topics across the social science and computer science academic disciplines. In this work, we explored research pertaining to cyberbullying, conducted across disciplines. We mainly sought to understand scholarly activity on intelligence techniques for the detection of cyberbullying when it occurs. Our findings suggest that the vast majority of academic contributions on cyberbullying focus on understanding the phenomenon, risk factors, and threats, with the prospect of suggesting possible protection strategies. There is less work on intelligence techniques for the detection of cyberbullying when it occurs, while currently deployed algorithms seem to detect the problem only up to some degree of success. The article summarises the current trends aiming to encourage discussion and research with a new scope; we call for more research tackling the problem by leveraging statistical models and computational mechanisms geared to detect, intervene, and prevent cyberbullying. Coupling intelligence techniques with specific web technology problems can help combat this social menace. We argue that a multidisciplinary approach is needed, with expertise from human–computer interaction, psychology, computer science, and sociology, for current challenges to be addressed and significant progress to be made.

ARTICLE HISTORY

Received 1 November 2017
Accepted 22 January 2018

KEYWORDS

Cyberbullying; internet bullying; cyber aggression; bullying; social media; literature survey

1. Introduction

Definitions and concepts of cyberbullying abound. Perhaps one of the most widely accepted definitions comes from Smith et al. (2008) defining 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’ (376). Generally speaking, cyberbullying can be seen as any form of abusive behaviour in the cyberspace. A typology of cyberbullying behaviour has been proposed by Nocentini et al. (2010) and includes four types of activity: written-verbal behaviour (phone calls, text messages, e-mails, instant messaging, chats, blogs, social networking communities, and websites), visual behaviour (posting, sending, or sharing compromising pictures and videos through the mobile phone or the internet), exclusion (purposefully excluding someone from an online group), and impersonation (stealing and revealing personal information, using another person’s name and account).

The rapid evolution and use of online social networks (OSNs) and the ever-increasing number of adolescents

admitting to have experienced cyberbullying, either as bullies, victims, or bystanders, create an alarming need for advancing research and development in this area. A study by Hinduja and Patchin (2015) surveyed a random sample of 457 students, aged 11–15, from a middle school in the Midwestern United States; approximately 34% of the students reported experiencing cyberbullying. An increase in cyberbullying can be noted, compared to previous results from the same authors (Hinduja and Patchin 2013) with a random sample of 4441 students (aged 10–18) from 37 schools in a large district in the southern United States; in this study, 20% of the students had reported experiencing cyberbullying in their lifetimes. Furthermore, the Cyberbullying Research Center (2015) studied the phenomenon in nine (random sampling) studies conducted between 2006 and 2015 reporting that, on average, 26% of the students had been the victim of cyberbullying at some point in their lifetime, while 16% of them admitted they had cyberbullied others at some point in their lifetime. Research has demonstrated a number of negative effects of

cyberbullying victimisation including lower self-esteem, frustration, depression, and anxiety, among others (Blumenfeld and Cooper 2010; Schrock and Boyd 2011; Smith-Ross et al. 2014). When the victim fails to cope with the emotional tension of the abuse, the consequences of cyberbullying become even more serious, leading to suicidal thoughts and behaviour (Foody, Samara, and Carlbring 2015; Schneider et al. 2012).

There is no doubt cyberbullying has become a social menace in the twenty-first century that needs to be addressed and combated. Yet, while there is an increasing flow of media stories reporting cases of cyberbullying, particularly within online social media, research efforts in the academic community are scattered over different topics across the social science and computer science academic disciplines. In this work, we explored research pertaining to cyberbullying, conducted across disciplines, aiming to understand scholarly activity on intelligence techniques for the detection of cyberbullying when it occurs. A similar piece of work has not been detected during our search of the literature; therefore, we hope this article will encourage discussion and research with this specific scope.

2. Search methodology

We first compiled a corpus of research on cyberbullying using keyword search in scientific databases of social science, humanities, and computer science (e.g. fields of human-computer interaction, psychology, computer science, and sociology). All scientific databases available to the authors through the University libraries as well as Google Scholar were searched for full-text, peer-reviewed manuscripts. A taxonomy of the cyberbullying key-terms has been presented by Al Mazari (2013), which includes the terms cyber-bullying/cyberbullying, cyber-grooming/cybergrooming, cyber-stalking/cyberstalking, electronic bullying, sms bullying, mobile bullying, online bullying, digital bullying, e-bullying, and internet bullying. This taxonomy formed our basic keyword search, which was expanded to include additional terms based on the keywords and ideas presented in the manuscripts themselves, such as predator, victim, bystander, harassment, trolling, aggressive behaviour, distressed behaviour, hate speech, content monitoring, doxing, and cybermobbing. Last, based on the scope of the review, the keywords 'intelligence techniques', 'detection', and 'intervention' were present on our searches, which significantly limited the corpus under study (approximately $N=200$ manuscripts). After careful reading of these manuscripts, we attempted to summarise the current trends in order to offer a practical proposal for future research with a more limited scope.

3. Practical recommendations based on major findings

3.1. Conduct more natural experiments across OSN platforms

Three kinds of research designs appear in the cyberbullying literature. Quantitative and qualitative inquiry is concerned with efforts from the social sciences, mainly focused on the participants' perceived experiences of being engaged in cyberbullying as predators, victims, or bystanders. Experimental designs are less frequent; in this case, researchers rely on experimental conditions studying cyber-bystander behaviour only. Our practical recommendation calls for more natural experiments with real-life OSNs data across platforms.

3.1.1. Quantitative and qualitative inquiry

The vast majority of cyberbullying research relies on self-reported measures. Social sciences quantitative survey research can help document the prevalence of cyberbullying as well as the relationship between cyberbullying penetration and various risk factors. In this case, respondents are mainly asked whether they have been the victim, perpetrator, or bystander of cyberbullying in general or through specific electronic means. For example, Baldry, Farrington, and Sorrentino (2017) examined different types of involvement in cyberbullying based on a survey of 2785 Italian students (aged 11–17) who self-reported about school and cyberbullying as victims and/or perpetrators. In another study, based on a sample of 1963 American middle school students, Hinduja and Patchin (2010) examined the relationship between middle school students' experience with cyberbullying and their level of self-esteem. A follow-up study by the same authors examined perceptions of, and experiences with, bullying, cyberbullying, and electronic teen dating violence, based on 1204 American middle- and high-school students (Hinduja and Patchin 2017). Although survey research is powerful in providing population-representative data, it is also associated with concerns such as the issue of social desirability in responses, the personal interpretations of global items, and the discrepancy between declaration and actual behaviour (Coughlan, Cronin, and Ryan 2009). Fewer studies follow a qualitative paradigm, using focus groups and interviews for an in-depth examination of participants' views and experiences of cyberbullying. For example, Vandebosch and Van Cleemput (2008) analysed qualitative data from 53 focus groups with students 10- to 18-years-old, showing how youngsters often interpret cyberbullying and associate the phenomenon with a wide range of practices that are intended to hurt (by the perpetrator) and perceived as hurtful (by the victim). Although qualitative

injury enables deep insights into the phenomenon, it does not come without limitations (Patton 1999).

3.1.2. Experimental designs

Experimental designs in cyberbullying research are less frequent. Our review failed to locate any experiments of cyberbullying predator and victim behaviour. Yet, a few social scientists seem to have employed experimental designs to study cyber-bystanders. In particular, Barlinska, Szuster, and Winiewski (2013) explored conditions of online vs. face-to-face cyberbullying, and public vs. private violence, using ‘simulated’ cyberbullying events inspired by actual cases reported at helpline.org.pl. A total of 760 students participated, each receiving a ‘message from a peer’ containing humiliating content (e.g. manipulated image showing a boy’s face on the body of a dog, saying ‘Hi, this is my classmate, he looks like a total fool.’). The study reported some interesting findings in regard to bystander behaviour, including that the cyberspace (compared to face-to-face contact) increased the likelihood of negative bystander behaviour, public violence (compared to private) was more likely to elicit negative bystander behaviour, and previous experience of cyberbullying increased the probability of negative bystander behaviour. Similarly, Obermaier, Fawzi, and Koch (2014) exposed participants to a cyberbullying scenario in a university Facebook group, in order to understand bystander behaviour. Results showed that a very severe cyberbullying incident boosted individuals’ intention to intervene, while a larger number of bystanders in a cyberbullying incident, rather than just a few, made participants feel less responsible and less willing to intervene, consistent with Barlinska, Szuster, and Winiewski’s (2013) findings on public violence. Last, in a study by Dillon and Bushman (2015), the participants were deceived to believe that they witnessed cyberbullying in the chatroom of an online support system for research surveys; the ‘victim’ stated difficulty with a survey question, which elicited an aggressive response from the chat monitor (bully). Results confirmed the researchers’ hypothesis that cyber-bystanders need to notice the cyberbullying event in order to intervene; indeed, those who noticed were four times more likely to intervene compared to those who did not notice. Also, direct cyber-bystander intervention was in the form of providing technical assistance to the victim as well as attacking the chat monitor reminding him of his duty to assist participants (Dillon and Bushman 2015).

3.1.3. Natural experiments

Natural experiments (i.e. empirical studies in real-life settings) occupy a smaller, but increasing, body of the cyberbullying literature. Working with real OSN data, a

few researchers have focused on the detection of cyberbullying when it occurs. This work derives mainly from the computer science area, implementing algorithms and methods that can identify the presence of cyberbullying terms and classify cyberbullying activity in OSNs. Yet, current algorithms seem to detect the problem only up to some degree of success, making it difficult to move into computational mechanisms for intervention and prevention of cyberbullying. For example, Dinakar, Reichart, and Lieberman (2011) developed a system for detecting textual cyberbullying in stand-alone posts in a dataset of YouTube comments. The system classified each comment in a range of sensitive topics such as sexuality, race, and intelligence, with 66% accuracy for the merged dataset. Similarly, Nandhini and Sheeba (2015) developed a system for detecting cyberbullying activities in OSNs and classifying terms as flaming, harassment, racism, and terrorism, with accuracy 87% in a MySpace dataset and 86% in a Formspring.me dataset. Another machine learning system was proposed by McGhee et al. (2011) detecting the occurrence of sexual violence with 68% accuracy in chat transcripts from the Perverted Justice database (<http://www.perverted-justice.com/>). Furthermore, considering dynamic, streaming (rather than static) data with insufficient labels, Nahar et al. (2014) devised a technique for automatic detection of cyberbullying in OSNs. Their experiments demonstrated that their technique outperformed the traditional methods used for cyberbullying detection. Last, a notable approach was considered by Potha and Maragoudakis (2014) applying data mining to the detection of cyberbullying. The study focused on understanding the strategies used by online sexual predators in their efforts to develop relationships with minors. The authors utilised a dataset of real-world dialogues (pairs of questions and answers between cyberpredator and the victim) in which time series was considered and severity was captured via behavioural patterns beyond signs of swearing and offending language. Results demonstrated satisfactory performance of the method for a few test-scenarios, but not for all. Overall, although some progress has been made, detecting cyberbullying when it occurs and identifying predators and their victims in real computer-mediated communication remains an open issue to be solved before intervention and prevention methods can be addressed.

3.1.4. Practical recommendation 1

A practical recommendation for future research would be to conduct more natural experiments with real-life OSNs data to track and understand the behaviour of predators and their victims in space and time. Real cyberbullying activity abounds in today’s cyberspace.

Different OSNs platforms might encourage or inhibit cyberbullying for different reasons. For example, it is possible that the severity of cyberbullying is linked to the degree of platform anonymity. This idea is linked to Suler's (2004) work, arguing that, while online, people may act out more frequently and intensively compared to how they behave in person, while different computer-mediated environments may facilitate diverse expressions of self. Today's easy access to data from various online social media platforms (e.g. Instagram, 4chan, Twitter, TwitchTV, Facebook, Snapchat) allows researchers to conduct natural experiments and to juxtapose patterns of behaviour and thus, consider causal relationships between factors such as (platform) anonymity and severity of cyberbullying.

3.2. Extend the operational definition and dimensions of cyberbullying research

Defining, measuring, or detecting specific cyberbullying behaviour is not a trivial task. Existing definitions of cyberbullying, as well as the one adhered in this review by Smith et al. (2008), often incorporate the criteria of traditional bullying such as repetition over time and imbalance of power (a victim who cannot easily defend him/herself). However, due to the unique nature of cyber-based communication, it is difficult to identify such criteria in the cyber abuse (Corcoran, Guckin, and Prentice 2015). As a result, there is uncertainty regarding the operational definition of cyberbullying and how to effectively measure it (Corcoran, Guckin, and Prentice 2015). On that note, Hosseinmardi et al. (2015) argued that most works on cyberbullying, as claimed by the original authors, are in fact more accurately described as research on cyberaggression, as they do not take into account the frequency of the event and the imbalance of power. We indeed found that factors such as severity (level of insult and duration) and power are yet to be considered in the operational definition of cyberbullying and therefore cyberbullying research, although their importance has been discussed in some social sciences research.

3.2.1. The power dimension

Although a central aspect of most operational definitions of traditional bullying, 'power' is difficult to determine in the cyber context (Corcoran, Guckin, and Prentice 2015). Is 'power' the ability to remain anonymous in the cyberspace (Smith et al. 2008)? Is it the ability to demonstrate superior technological knowledge (Vandebosch and Van Cleemput 2009)? Is it the immediacy of content dissemination and capacity to humiliate on a grand scale (Langos 2012)? Or is 'power' the perceived

popularity of the predator causing more psychological distress? The latter was investigated by Pieschl et al. (2013), who found that, compared to being harassed by an unpopular cyberbully, being harassed by a popular cyberbully was more distressing and elicited more negative mood and helplessness. Understanding what 'power' in cyberspace entails will significantly inform the operational definition of cyberbullying.

3.2.2. The dimension of severity – duration and level of insult

Cyberbullying can occur anytime and anywhere and is believed to be more damaging than traditional face-to-face bullying because of the fluidity and frequency of the bullying behaviour using technology. In fact, several authors (e.g. Langos 2012; Sticca and Perren 2013) hypothesised that because bullying acts performed online are visible for a long(er) period of time and to a large audience (who may also join the bully), their negative effects can be more severe and longer lasting, compared to victims of repeated (offline) bullying acts. Yet, there is lack of empirical research tackling cyberbullying as a sequence of actions that involve repetition of harming content and levels of severity. Potha and Maragoudakis (2014) seem to be the first to have considered the duration and level of insult in cyberbullying; using a dynamic time warping algorithm, they were able to provide an immediate indicator for the severity of cyberbullying within a given dialogue. Yet, more research is needed for understanding (and detecting) the level of insult and duration of the cyber abuse.

3.2.3. The anonymity dimension

The anonymity in cyberbullying adds a totally new dimension to the nature of traditional bullying. The devices that are used (such as mobile phones and computers) make it easier for a perpetrator to act anonymously (e.g. by using a nickname) and without directly facing the victim (Slonje, Smith, and Frisen 2013; Sticca and Perren 2013). Moreover, cyberbullies have less chance of getting caught or punished as they can perpetrate without adult supervision (Smith et al. 2008). What makes the anonymity dimension more apparent in cyberbullying is the evidence that many cyberbullies do not choose in-person bullying if the cyber route is denied. As Englander (2012) discussed, cyberbullies might not bully in person because they feel powerless socially or because they are invested in school and academics, but are willing to bully online because they believe that cyberbullying is without risk since adults are not present. It is therefore plausible that the degree of platform anonymity can promote or inhibit cyberbullying behaviour. This hypothesis brings up the question:

Are predators willing to attack their victims online, if the platform does not warrant their anonymity? Looking at cyberbullying in relation to the degree of platform anonymity might inform its measurement and detection across various OSNs.

3.2.4. Practical recommendation 2

A practical recommendation for future research would be to inform and extend the operational definition and thus, measurement and detection of cyberbullying. Factors such as severity (level of insult and duration) and power are yet to be considered seriously in cyberbullying research. Valuable insight could emerge from research that tackles whole blocks of cyberbullying activity in OSNs, demonstrating and understanding the evolution, repetition, and imbalance of power evident in these events. Current algorithms seem to detect the problem only up to some degree of success; we would argue that consideration of these factors might improve their intelligence.

3.3. Backtrack cyberbullying behaviour and consider culture

A consistent profile of all actors involved in the phenomenon has yet to be presented by researchers of cyberbullying and it appears to be a demanding area for exploration. A typology of cyberbullying actors in terms of their personal characteristics has yet to be presented in the cyberbullying literature. There is limited research on how cyberbullying begins, feeds on, and evolves through time. There is also limited research on the bully-victim as an actor of cyberbullying, although an alarming consideration, emerging from social sciences research, is that a bullied person can become a bully. We suggest that computer science algorithms can help backtrack cyberbullying behaviour looking at these issues profiles, typologies, and behaviours as they get formed and evolve. A multi-cultural approach to cyberbullying can also inform algorithmic approaches to detection.

3.3.1. The profiles of the main actors

There are three main actors in the cyberbullying menace: the predator or cyberbully, the cybervictim, and the bystander. A consistent profile of all actors is yet to be presented.

Predator/cyberbully. In an overview of research on the types of cyberbullies (also cyberbullying perpetrators or predators), Kyriacou and Zuin (2016) identified five main categories, taking into account the psychological attributes (both personal and social) that underpin their behaviour: the sociable cyberbully (cyberbullying for fun in order to entertain his/her friends without

serious consideration of the victim's feelings); the lonely cyberbully (a relatively isolated cyberbully with no friends, spends his/her time by abusing others with whom s/he has little or no personal contact); the narcissistic cyberbully (a cyberbully demonstrating power by administering harm to another person); the sadistic cyberbully (a cyberbully enjoying causing distress, harm, and suffering to another person); and the morally driven cyberbully (a cyberbully feeling the victim is receiving justice for his/her actions). Additionally, in a survey research, Korean, You and Lim (2016) used a sample of 3449 middle school students and demonstrated a set of variables associated with more cyberbullying perpetration, particularly longer use of the internet, more previous bullying and victim experiences, a higher aggression level, and lack of self-control.

Cybervictim. Much of the previous research has attempted to identify risk factors for bullying and cyberbullying (typically examined together) focusing on demographic and behavioural measures. A number of psychological variables emerged in different studies describing the cybervictim. Sourander et al. (2010) for example, found that cybervictim status was associated with living with non-parental caregivers (i.e. non-biological parents), perceived emotional and peer problems, and feeling unsafe at school, while in Schneider et al. (2012) cybervictims reported lower school performance and school attachment.

Bystander. The third actor in cyberbullying is the (negative) bystander who observes bullying without taking action. A comprehensive study of this actor comes from Barlinska, Szuster, and Winiewski (2013), who found that three factors increased the likelihood of negative bystander behaviour: (i) the cyberspace, meaning that negative bystander behaviour occurs more often in the cyberspace than offline, (ii) the private nature of the act, meaning that bystander behaviour might occur more frequently in private forms of violence, and (iii) the experience of being a cyberbullying predator seems to be an important predictor of negative bystander behaviour. Two factors seem to decrease negative bystander behaviour: (i) affective empathy, i.e. the ability to understand the emotions of others, and (ii) cognitive empathy, i.e. the ability to anticipate the consequences of one's actions on others (Barlinska, Szuster, and Winiewski 2013).

3.3.2. A typology of cyberbullying actors

Findings are sparse and inconsistent, calling for more work in this area. Gender, age, sexual orientation, and other personal characteristics such as the use of a computer, school performance, and past experiences with bullying seem to relate to the bullying phenomenon.

3.3.2.1. Gender. Inconsistent findings have been reported regarding gender. Although research on traditional bullying shows that bullying is more common among boys, as discussed in Sanchez et al. (2016), for cyberbullying, findings are mixed. Several studies report that males are indeed more likely to be cyberbullies than their female counterparts (Lapidot-Leffler and Dolev-Cohen 2015; Li 2006); yet, others report no gender differences (Patchin and Hinduja 2006) and others claim that girls outnumber boys (Keith and Martin 2005; Kowalski and Limber 2007). In a study of 2186 middle- and high-school students, Mishna et al. (2012) explored the factors that contribute to engagement with cyberbullying, looking at groups of actors including victims, bullies, bully-victims (both bully and be bullied online) and those not involved. Findings included that bully-victims were more likely to be females, while no gender differences were found among students who bullied others or who were victimised online. Moreover, in Schneider et al. (2012), a total of 20,406 students (9–12 grade) in MetroWest Massachusetts completed surveys assessing their bullying victimisation and psychological distress. The study showed that girls were more likely, than were boys, to report cyberbullying as predators, especially in combination with school bullying, but they were also more likely to be victims of both types of bullying (on school property and in cyberspace).

3.3.2.2. Age. While traditional bullying seems to peak during middle school, cyberbullying peaks somewhat later (Pabian and Vandebosch 2016). In fact, with age, there seems to be a gradual shift away from traditional forms of bullying such as spreading rumours, to cyberbullying; for example, Mishna et al. (2012) found that the older the student, the more likely s/he was to cyberbully others or to both bully and be bullied online, rather than to be a bully or victim. The majority of cyberbullying research conducted so far has focused on adolescents and teens, e.g. middle- and high-school students (e.g. Li 2010; Steffgen et al. 2011). Less research to date has investigated cyberbullying behaviour in young adults (Brack and Caltabiano, 2014; Hemphill and Heerde 2014). Last, very little cyberbullying research exists on primary school students (Tangen and Campbell 2010).

3.3.2.3. Sexual orientation. There seems to be a consistent finding that non-heterosexual individuals are targets of traditional bullying and cyberbullying. For example, Schneider et al. (2012) reported that non-heterosexual youths were more likely to be victims of cyberbullying, compared to heterosexuals (10.5% vs. 6.0%). A previous study reported similar findings, showings that Lesbian, Gay, Bisexual, Transgender (LGBT) individuals were

twice as likely to experience cyberstalking or e-mail harassment from a stranger, compared to heterosexual individuals (Finn 2004).

A few other profiles of cyberbullying actors have been reported in the literature as follows.

3.3.2.4. Computer use. Students who were victims, bullies, and bully-victims were more likely than students who were not involved in cyberbullying to use the computer for more hours a day and to give their password to friends (Mishna et al. 2012). Also, intensive use of the internet emerged as a risk factor for child cyber-harassment (Wolak, Mitchell, and Finkelhor 2007). Furthermore, the location of the computer at home was found to be a predictive factor of cyber victimisation. Children who use the computer in private places at their home (e.g. bedroom) were at higher risk to be victimised than children who used computers in a public space in their home (Sengupta and Chaudhuri 2011).

3.3.2.5. School performance. According to Schneider et al. (2012), youth who reported lower school performance and lower school attachment were also more likely to be victimised with cyberbullying; in particular, students who received mostly Ds and Fs were twice as likely to be victims of cyberbullying compared to students who received mostly As (11.3% vs. 5.2%).

3.3.2.6. Bullied person, bullying others. There is a lack of research on the bully-victim group (persons being bullied and also bullying others) while a potential causal link is alarming and warrants further investigation (Does bullied person become a bully and under what conditions?). For example, in their survey research, You and Lim (2016) found that previous offline bullying and victim experiences were associated with more cyberbullying. Similarly, Mishna et al. (2012) argued that the cyberspace offers an easy venue for ‘revenge’ or ‘payback’ with a high prevalence of bully-victim behaviour (26%) in a sample of 2186 participants (Mishna et al. 2012).

3.3.3. Practical recommendation 3

Overall, there is limited research on how cyberbullying begins, feeds on, and evolves through time. There is also limited research on the bully-victim as a separate actor of cyberbullying, although an alarming consideration, emerging from social sciences research, is that a bullied person can become a bully. Computer science algorithms can help backtrack cyberbullying behaviour looking at these issues, e.g. when and how one engages in bullying (e.g. person acting properly, then bullies after being bullied). Furthermore, a multi-cultural approach should be considered. The typology of

cyberbullying participants in terms of gender, age, sexual orientation, and other characteristics should involve cultural elements, which might be the cause of inconsistent research findings regarding these factors. Similarly, cyberbullying actors – predator, victim, and bystander – might possess different profiles across cultures. A multi-cultural approach to cyberbullying could generate further useful insights into advancing these typologies. This appears to be an understudied, yet, demanding area for exploration in the social sciences, which can greatly inform algorithmic approaches to detection and prevention from a computer science perspective.

3.4. Build synergies between researchers in humanities and computers science

This paper explored research pertaining to cyberbullying across disciplines, from social science and humanities to computer science. Our last recommendation would be to begin the dialogue between social science/humanities and computer science. Communication between disciplines is virtually non-existent within the cyberbullying arena. Although computer scientists do reference outcomes of social sciences work (the opposite is rare), it is mostly done with the prospect of demonstrating knowledge gaps, rather than engaging in true dialogue. There is an immediate need for more research attacking the problem from the perspective of statistical models and computational mechanisms for detection, intervention, and prevention of cyberbullying. The authors would argue that the latter needs the attention and close collaboration of both communities, particularly people with expertise from human-computer interaction, psychology, computer science, and sociology, for current challenges to be addressed and significant progress to be made.

4. Conclusion

While there is an increasing flow of media stories reporting cases of cyberbullying, particularly within online social media, research efforts in the academic community are scattered over different topics and across the humanities and computer science. Overall, it appears, research on cyberbullying is still in its infancy and most studies are mere reports of prevalence rates and relationships among variables. The majority of academic contributions focus on understanding the phenomenon, risk factors, and threats with the prospect of suggesting possible protection strategies. Detecting cyberbullying when it occurs and identifying predators and their victims in real computer-mediated communication remains an open issue to be solved before intervention and

prevention methods can be addressed. We have presented a few recommendations for future research, which have been developed through our analyses. Coupling intelligence techniques with specific web technology problems can help combat this social menace. Recognising blocks of cyberbullying activity and understanding dimensions such as duration, severity, power, and anonymity can shed valuable insights into how cyberbullying is fed and evolves. There is an immediate need for true multidisciplinary work between social and computer sciences and we are confident that articles will serve as a multidisciplinary agenda to guide future research in this area.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work is partially funded by the EC project ‘ENCASE (ENhancing seCurity and privAcY in the Social wEb): a user-centred approach for the protection of minors’ under the contract H2020-MSCA-RISE-2015-691025.

ORCID

Andri Ioannou  <http://orcid.org/0000-0002-3570-6578>

References

- Al Mazari, A. 2013. “Cyber-bullying Taxonomies: Definition, Forms, Consequences and Mitigation Strategies.” In *5th International Conference on Computer Science and Information Technology (CSIT)*, Amman, Jordan, 126–133. IEEE.
- Baldry, A. C., D. P. Farrington, and A. Sorrentino. 2017. “School Bullying and Cyberbullying among Boys and Girls: Roles and Overlap.” *Journal of Aggression, Maltreatment & Trauma* 26 (9): 937–951.
- Barlinska, J., A. Szuster, and M. Winiewski. 2013. “Cyberbullying among Adolescent Bystanders: Role of the Communication Medium, Form of Violence, and Empathy.” *Journal of Community & Applied Social Psychology* 23 (1): 37–51.
- Blumenfeld, W. J., and R. M. Cooper. 2010. “LGBT and Allied Youth Responses to Cyberbullying: Policy Implications.” *The International Journal of Critical Pedagogy* 3 (1): 112.
- Brack, K., and N. Caltabiano. 2014. “Cyberbullying and Self-esteem in Australian Adults.” *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 8 (2). doi:10.5817/CP2014-2-7.
- Corcoran, L., C. M. Guckin, and G. Prentice. 2015. “Cyberbullying or Cyber Aggression? A Review of Existing Definitions of Cyber-Based Peer-to-Peer Aggression.” *Societies* 5 (2): 245–255.

- Coughlan, M., P. Cronin, and F. Ryan. 2009. "Survey Research: Process and Limitations." *International Journal of Therapy & Rehabilitation* 16 (1): 9–15.
- Cyberbullying Research Center. 2015. *Summary of Our Cyberbullying Research (2004–2015)*. Accessed July 2015. <http://cyberbullying.org/summary-of-our-cyberbullying-research>.
- Dillon, K. P., and B. J. Bushman. 2015. "Unresponsive or Unnoticed? Cyberbystander Intervention in an Experimental Cyberbullying Context." *Computers in Human Behavior* 45: 144–150.
- Dinakar, K., R. Reichart, and H. Lieberman. 2011. "Modeling the Detection of Textual Cyberbullying." *The Social Mobile Web* 11: 02.
- Englander, E. 2012. *Spinning our Wheels: Improving our Ability to Respond to Bullying and Cyberbullying*. Child & Adolescent Psychiatric Clinics of North America.
- Finn, J. 2004. "A Survey of Online Harassment at a University Campus." *Journal of Interpersonal Violence* 19 (4): 468–483.
- Foody, M., M. Samara, and P. Carlbring. 2015. "A Review of Cyberbullying and Suggestions for Online Psychological Therapy." *Internet Interventions* 2 (3): 235–242.
- Hemphill, S. A., and J. A. Heerde. 2014. "Adolescent Predictors of Young Adult Cyberbullying Perpetration and Victimization among Australian Youth." *Journal of Adolescent Health* 55 (4): 580–587.
- Hinduja, S., and J. W. Patchin. 2013. "Social Influences on Cyberbullying Behaviors among Middle and High School Students." *Journal of Youth and Adolescence* 42 (5): 711–722.
- Hinduja, S., and J. W. Patchin. 2015. *Cyberbullying Legislation and Case Law: Implications for School Policy and Practice*. Cyberbullying Research Center.
- Hinduja, S., and J. W. Patchin. 2017. "Cultivating Youth Resilience to Prevent Bullying and Cyberbullying Victimization." *Child Abuse & Neglect* 73: 51–62.
- Hinduja, S., and J. W. Patchin. 2010. "Bullying, Cyberbullying, and Suicide." *Archives of Suicide Research* 14 (3): 206–221.
- Hosseinmardi, H., S. A. Mattson, R. I. Rafiq, R. Han, Q. Lv, and S. Mishra. 2015. *Detection of Cyberbullying Incidents on the Instagram Social Network*. arXiv preprint arXiv:1503.03909.
- Keith, S., and M. E. Martin. 2005. "Cyber-bullying: Creating a Culture of Respect in a Cyber World." *Reclaiming Children and Youth* 13 (4): 224.
- Kowalski, R. M., and S. P. Limber. 2007. "Electronic Bullying among Middle School Students." *Journal of Adolescent Health* 41 (6): S22–S30.
- Kyriacou, C., and A. Zuin. 2016. "Cyberbullying and Moral Disengagement: An Analysis Based on a Social Pedagogy of Pastoral Care in Schools." *Pastoral Care in Education* 34 (1): 34–42.
- Langos, C. 2012. "Cyberbullying: The Challenge to Define." *Cyberpsychology, Behavior, and Social Networking* 15 (6): 285–289.
- Lapidot-Lefler, N., and M. Dolev-Cohen. 2015. "Comparing Cyberbullying and School Bullying among School Students: Prevalence, Gender, and Grade Level Differences." *Social Psychology of Education* 18 (1): 1–16.
- Li, Q. 2006. "Cyberbullying in Schools: A Research of Gender Differences." *School Psychology International* 27 (2): 157–170.
- Li, Q. 2010. "Cyberbullying in High Schools: A Study of Students' Behaviors and Beliefs About This New Phenomenon." *Journal of Aggression, Maltreatment & Trauma* 19 (4): 372–392.
- McGhee, I., J. Bayzick, A. Kontostathis, L. Edwards, A. McBride, and E. Jakubowski. 2011. "Learning to Identify Internet Sexual Predation." *International Journal of Electronic Commerce* 15 (3): 103–122.
- Mishna, F., M. Khoury-Kassabri, T. Gadalla, and J. Daciuk. 2012. "Risk Factors for Involvement in Cyber Bullying: Victims, Bullies and Bully-victims." *Children and Youth Services Review* 34 (1): 63–70.
- Nahar V., S. Al-Maskari, X. Li, and C. Pang. 2014. "Semi-supervised Learning for Cyberbullying Detection in Social Networks." In *Databases Theory and Applications, ADC, Lecture Notes in Computer Science*, edited by H. Wang, and M. A. Sharaf, Vol. 8506, 160–171. Cham: Springer.
- Nandhini, B. S., and J. I. Sheeba. 2015. "Online Social Network Bullying Detection Using Intelligence Techniques." *Procedia Computer Science* 45: 485–492.
- Nocentini, A., J. Calmaestra, A. Schultze-Krumbholz, H. Scheithauer, R. Ortega, and E. Menesini. 2010. "Cyberbullying: Labels, Behaviours and Definition in Three European Countries." *Australian Journal of Guidance and Counselling* 20 (02): 129–142.
- Obermaier, M., N. Fawzi, and T. Koch. 2014. "Bystanding or Standing By? How the Number of Bystanders Affects the Intention to Intervene in Cyberbullying." *New Media & Society*. doi:10.1177/1461444814563519.
- Pabian, S., and H. Vandebosch. 2016. "An Investigation of Short-Term Longitudinal Associations Between Social Anxiety and Victimization and Perpetration of Traditional Bullying and Cyberbullying." *Journal of Youth and Adolescence* 45 (2): 328–339.
- Patchin, J. W., and S. Hinduja. 2006. "Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying." *Youth Violence and Juvenile Justice* 4 (2): 148–169.
- Patton, M. Q. 1999. "Enhancing the Quality and Credibility of Qualitative Analysis." *Health Services Research* 34 (5 Pt 2): 1189.
- Pieschl, S., T. Porsch, T. Kahl, and R. Klockenbusch. 2013. "Relevant Dimensions of Cyberbullying—Results From Two Experimental Studies." *Journal of Applied Developmental Psychology* 34 (5): 241–252.
- Potha, N., and M. Maragoudakis. 2014. "Cyberbullying Detection Using Time Series Modeling." In *2014 IEEE International Conference on Data Mining Workshop, Shenzhen, China*, 373–382. IEEE.
- Sanchez, F. C., M. F. Romero, J. Navarro-Zaragoza, A. L. Ruiz-Cabello, O. R. Frantzisko, and A. L. Maldonado. 2016. "Prevalence and Patterns of Traditional Bullying Victimization and Cyber-Teasing Among College Population in Spain." *BMC Public Health* 16 (1): 1.
- Schneider, S. K., L. O'Donnell, A. Stueve, and R. W. Coulter. 2012. "Cyberbullying, School Bullying, and Psychological Distress: A Regional Census of High School Students." *American Journal of Public Health* 102 (1): 171–177.
- Schrock, A., and D. Boyd. 2011. "Problematic Youth Interaction Online: Solicitation, Harassment, and Cyberbullying." *Computer-mediated Communication in Personal Relationships*, edited by Kevin B. Wright, and Lynn M. Webb, 368–398. New York: Peter Lang.

- Sengupta, A., and A. Chaudhuri. 2011. "Are Social Networking Sites a Source of Online Harassment for Teens? Evidence from Survey Data." *Children and Youth Services Review* 33 (2): 284–290.
- Slonje, R., P. K. Smith, and A. Frisen. 2013. "The Nature of Cyberbullying, and Strategies for Prevention." *Computers in Human Behavior* 29 (1): 26–32.
- Smith, P. K., J. Mahdavi, M. Carvalho, S. Fisher, S. Russell, and N. Tippett. 2008. "Cyberbullying: Its Nature and Impact in Secondary School Pupils." *Journal of Child Psychology and Psychiatry* 49 (4): 376–385.
- Smith-Ross, C., A. Esmail, A. Omar, and K. Franklin. 2014. "Chapter Nine Bullying: Recognizing the Warning Signs." In *Alleviating Bullying: Conquering the Challenge of Violent Crimes*, edited by A. Esmail, 146–160. Lanham, MD: University Press of America, Inc.
- Sourander, A., A. B. Klomek, M. Ikonen, J. Lindroos, T. Luntamo, M. Koskelainen, Terja Ristkari, and H. Helenius. 2010. "Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents." *Archives of General Psychiatry* 67 (7): 720–728.
- Steffgen, G., A. Koenig, J. Pfetsch, and A. Melzer. 2011. "Are Cyberbullies Less Empathic? Adolescents' Cyberbullying Behavior and Empathic Responsiveness." *Cyberpsychology, Behavior, and Social Networking* 14 (11): 643–648.
- Sticca, F., and S. Perren. 2013. "Is Cyberbullying Worse than Traditional Bullying? Examining the Differential Roles of Medium, Publicity, and Anonymity for the Perceived Severity of Bullying." *Journal of Youth and Adolescence* 42 (5): 739–750.
- Suler, J. 2004. "The Online Disinhibition Effect." *Cyberpsychology & Behavior* 7 (3): 321–326.
- Tangen, D., and M. Campbell. 2010. "Cyberbullying Prevention: One Primary School's Approach." *Australian Journal of Guidance and Counselling* 20 (02): 225–234.
- Vandebosch, H., and K. Van Cleemput. 2008. "Defining Cyberbullying: A Qualitative Research Into the Perceptions of Youngsters." *CyberPsychology & Behavior* 11 (4): 499–503.
- Vandebosch, H., and K. Van Cleemput. 2009. "Cyberbullying among Youngsters: Profiles of Bullies and Victims." *New Media & Society* 11 (8): 1349–1371.
- Wolak, J., K. J. Mitchell, and D. Finkelhor. 2007. "Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts." *Journal of Adolescent Health* 41 (6): S51–S58.
- You, S., and S. A. Lim. 2016. "Longitudinal Predictors of Cyberbullying Perpetration: Evidence from Korean Middle School Students." *Personality and Individual Differences* 89: 172–176.