Managing Cyber-bullying in Online Educational Virtual Worlds

Diego Fernando Gutierrez Aponte
Department of Computing
Macquarie University
North Ryde, NSW, 2109, AUSTRALIA
diegovillavo@gmail.com

Deborah Richards
Department of Computing
Macquarie University
North Ryde, NSW, 2109, AUSTRALIA
+61(2)98509567
deborah.richards@mq.edu.au

ABSTRACT
Online Educational Virtual Worlds offer promise that is currently not being realised because of potential threats to the child's safety and wellbeing. This paper seeks to better understand the behavioural and psychological issues, particularly relating to cyber-bullying, faced by school children when they are online and what solutions currently exist. As an outcome of this understanding we make recommendations regarding how cyber-bullying should be managed in educational virtual worlds taking a hybrid approach involving policy, technology and non-technology based solutions.

Categories and Subject Descriptors
H.5.1 [**Multimedia Information Systems**]: Artificial, augmented, and virtual realities, Audio input/output K.4 COMPUTERS AND SOCIETY K.4.0 General K.4.1 [**Public Policy Issues**]: Abuse and crime involving computers, Human safety, Privacy, Use/abuse of power.

General Terms
Design, Human Factors, Legal Aspects.

Keywords
eSafety, cyber-bullying, cyber-victim, educational virtual worlds.

1. INTRODUCTION
Online Educational Virtual Worlds (VWs) offer promise that is currently not being realised in our schools. The key reason for this given by Education Departments and schools with whom we have spoken are concerns around student safety and wellbeing. Remarkably in other application domains virtual worlds are seen as a way to create safe and low risk environments [7]. This is certainly true when it comes to the use of virtual worlds in serious games and training simulations in the adult world, such as train and aircraft simulators and military or first responder scenario-based training environments. The safety issues identified by schools are broad and include access to inappropriate material, student privacy and appropriate behaviour. In this paper, we will narrow our focus to online behaviours, particularly cyber-bullying, in educational virtual worlds and the broader context of the Internet.

IE'2013, September 30 - October 01 2013, Melbourne, VIC, Australia

http://dx.doi.org/10.1145/2513002.2513006

The Internet allows users to learn, to have fun, to research, to meet people, to build friendships, and to search for information. Within the Internet are virtual worlds where virtual environments with different scenarios and avatars interact to achieve common or individual goals. The avatars may represent users and be controlled by them. Crystal [8, p. 12] defined virtual words as "imaginary environments which people can enter to engage in text-based fantasy social interaction". It is in these virtual worlds that the continued exchange of communication between two or more people can become problematic if the presence of inappropriate online behaviour results in harm to at least one of the parties. Such situations have psychological aspects that generate distress and embarrassment to potential cyber-victims.

In a detailed analysis of problematic online youth solicitation, harassment, and cyberbullying, Schrock and Boyd [26,p.30) state:

> It is unclear if harassment on virtual worlds is inherently more distressing than other online technologies. Gamers may have a greater connection with their avatars, and may even feel that an avatar is physically their own body, raising the question of if people playing MMOs are more susceptible to psychological harm through griefing.

Nevertheless, Boyd [3] notes that we have to be wary of an overreaction and moral panic to a situation (that is, teens being online and almost constantly digitally connected) that has partly come about due to "parental fears, over-scheduling, and lack of viable transportation often make offline socialization difficult, if not altogether impossible" (p.1).

It is good to remember that technology is not the problem; the problem is the misuse of the technology as an instrument to commit undesirable online actions that may harm others. That is why, in this paper, we (1) describe some problems related to misuse of educational and non-educational virtual worlds; (2) explain the consequences of these problems on children and teenagers (among others); (3) identify a range of current solutions; and finally (4) recommend a hybrid approach combining policy, technology and non-technology based solutions and set of features that should be considered in the design, development and deployment of online educational virtual worlds.

2. LITERATURE REVIEW – ISSUES AND CONSEQUENCES

This section provides a general literature review of inappropriate online (and some offline) behaviours by or to children. Two main parts are described in this section: (1) the issues and types of threats (such as cyber-bullying and cyber-threats), and (2) the consequences.

2.1 Behavioural Issues in Virtual Worlds

In this section, we first compare traditional bullying and cyber-bullying, followed by definitions of the latter. Then we present examples of types of cyber-bullying and introduce other forms of cyber-bullying such as cyber-stalking and cyber-threats.

2.1.1 Bullying and Cyber-bullying

Before proceeding to explain what "cyber-bullying" is, let us first explain what "bullying" is so that we can understand the differences. Bullying is a behaviour that usually takes place between two people. The person who attempts to physically or verbally hurt another person becomes the bully (or perpetrator), while the other person is called the victim. According to Kowalski, Limber, & Agatston [15], bullying is an imbalance of power or strength. Traditional bullying happens when, for example, a stronger male student in primary school dares another male student (who is younger or has less strength) to do some physical activity that the former is actually able to do and the latter may not be able to do. When bullies discover the weaknesses of others, they immediately start to target them. The intention is to demonstrate, perhaps, that they are superior in some aspects, or simply to make fun of their victims to cause embarrassment.

Apart from embarrassment—which is bad enough—violence is also involved when bullies experiment with aggressive behaviour (such as hitting, kicking and pushing), especially when stronger boys or girls try to intimidate their victims. The bully can do further harm, exacerbated by others, through rumour-spreading or gossiping. These rumours generate more taunting, social exclusion and manipulation of friendship—or shunning and are often an attack on the victim's speech and appearance [15]. One would imagine that a virtual world would provide safety from physical harm. Further, the ability to alter one's appearance and persona could even allow a person to avoid becoming a target. However, online virtual worlds introduce new threats.

A simple definition states that "cyber-bullying involves bullying through the use of technology such as the Internet and cellular phones" [14, p. 46]. Cyber-bullying may be seen as the evolution of bullying in an era of fast and constant communication. Another definition of cyber-bullying is "sending or posting harmful material or engaging in other forms of social aggression using the Internet or other digital technologies" [29, p. 1]. The Internet, for instance, never shuts down. We can therefore assume that cyber-bullying can be practiced all day long, any day, and at any time. McQuade, Colt, and Meyer [17] noted that digital bullying is spreading more rapidly, thanks to the ease provided by technology and the Internet. Many devices have features that support the viral spread of cyber-bullying. For instance, mobile network providers, allow their customers to send an instant message (IM), short message service (SMS) or images to one or more individuals and by accessing Wi-Fi hot spots users are able to connect to social networks such as Twitter and Facebook and send content with offensive or inflammatory comments and graphics to be displayed to all of a person's contacts or followers. Once the content is sent, even if it is later deleted from the website or forum it may have already spread among thousands of users and be stored on other computers.

Didden et al. [10], in their study of students with special needs, stated that there is a correlation between the amount of time using a computer and the risk of being a victim of online bullying or taking the role of a perpetrator. It was found that students using computers with Internet access for less than one hour per day were less likely to become victims of cyber-bullying, but that students using computers with Internet access for more than one hour per day were more likely to be victimized and/or become cyber-bullies [10].

In this evolution of bullying, bullies have new strategies to throw the rock and hide the hand. Rogers [23] describes that cyber-bullies take advantage of the fact that in social networks, chatrooms or forums, they do not have to reveal their real identity. When cyber-bullying, they can target people while not directly exposing themselves. This leads a cyber-bully to think that they cannot be caught and can continue as long as they please (p. 12).

Some interesting phenomena are emerging due to the ability to hide and role-play in the virtual world. The impact of one's behaviour may not be as apparent in the real world. As a result, some may be guilty of unwittingly causing or condoning harm to another, or they may not realise the extent of the harm they have caused. Yun-yin Huang & Chou [30] claim that a person with computing knowledge and access to the Internet could very easily send rumours or harassing emails; therefore, so can cyber-victims. This trend magnifies the problem and turns aggressive online behaviour into an endless chain. Rogers [23] stated that cyber-bullying, compared with bullying, is very different when young people target older people. Adults who might become targets of cyber-bullying by youths vary from teachers (mainly) to parents or other members of a community. Finally, Kowalski et al., [15] outlines some of the key signs to discover when a child is being cyber-bullied. Awareness of these signs may be useful for strategies to identify and deal with cyber-bullying. In short, the signs include when a child or teenager: 1) seems bothered during or after being connected to the Internet 2) looks upset after receiving an SMS or email. 3) suddenly stops social interaction with their peers or parents, or 4) receives a drop in performance in their school grades. We note that these symptoms mostly occur in the real world as a result of activity in the virtual world; requiring solutions to cyber-bullying in both worlds.

2.1.2 Types of Cyber-bullying

A number of types of cyber-bullying have been identified including: flaming; cyber-harassment; denigration; impersonation, masquerading, outing, trickery, ostracism and exclusion as described briefly below.

2.1.2.1 Flaming

This is an argument that generally takes place in chat rooms, or by posts or comments in a forum, social network, blog or even in games. Willard [29] described that this kind of cyber-bullying usually carries rude and vulgar language, insults that come and go, and (in some cases) threats between the participants. Note that while threats may occur in games like Halo or Gears of War, these threats do not represent intentions in real life. Flaming occurs sometimes in front of other users of the IM service, bystanders; who eventually join into an argument to heat up the discussion or

to extinguish the flames. Despite flaming occurring mainly in public environments, it can also happen in private spaces such as private chat rooms. Other types of non-public flaming can occur through email or instant messages that may be addressed to one person or group with no more recipients than intended. In brief flaming involves short-lived/term arguments, no repetition and exchange of aggressions between the parties.

2.1.2.2 Cyber-harassment and Griefing

Black's Law Dictionary defines cyber-harassment as "Words, conduct, or action (usually repeated or persistent) that being directed at a specific person, annoys, alarms, or causes substantial emotional distress in that person" [11, p.733]. Harassment is the repeated transmission of aggressive messages to a person or group. It becomes cyber harassment when virtual means are used for this purpose; for example, the constant sending of harmful words from a cyber-bully to a target through SMS or email. The channels used for cyber-harassment may be the same as in flaming. Email, IM and text messages are the most common methods used for this behaviour. Kowalski et al. [15] described 'griefers' as individuals who look to harass other players in multiplayer online games. Rather than seeking a win they want to ruin the experience of playing a game for other players, for example, repeatedly killing or teleporting the other's avatar [26]. In contrast to flaming, cyber-harassment is characterised by long-term and repeated aggression, where one side makes the aggression, and the other side tries to delete the aggression or respond to stop the cyber-harassment

2.1.2.3 Denigration

This sort of online behaviour is about choosing a person to make him/her the target of many different stories that denigrate their reputation and public image in front of others. For example, Kowalski et al. [15] related a story of a song that was modified by some teenagers shortly after being uploaded onto a website for other classmates to listen to it. The teens changed the lyrics to create a derogatory song about one of their classmates. Denigration is common, too, among cyber-bullies who try to ridicule an adult, such as a teacher, or spread false rumours.

2.1.2.4 Impersonation

This is when a cyber-bully basically steals confidential information about someone else (the cyber-bullied), and then accesses their email accounts, social networks, forums, games and virtual worlds [29]. The aim is to take over the cyber victim's accounts or devices, and to attempt to cause harm to them with comments and photos that their victim would never themselves have posted or uploaded. These harmful comments may be, for example, addressed to the cyber victim's friends. The messages are intended to upset the friends, who might then react against the victim with anger, and finish the friendship or turn into enemies.

2.1.2.5 Masquerading

This type of cyber-bullying conceals the identity of the cyber-bully with someone else's identity to avoid being caught with their own identity in order to avoid trouble; that is, the cyber-bully pretends to be another person so that they can cause distress to classmates or even closer friends [19, p. 1225]. One example of this issue is when a child or teen gives their password to their friends as a sign of friendship, and their friends use the account for cyber-bullying [19]. Another example is when a child is at a friend's house and leaves without first signing off from their email account. The other person is able to read and send emails to other people while hiding behind their friend's identity.

2.1.2.6 Outing

Willard [29] defined outing as the action of sending, posting and forwarding in a public way, any exchange of messages and images that have been intended just for one receiver and then, the latter publishes the material causing embarrassment. The author suggests that this aggressive online behaviour involves sexually suggestive or explicit photographs originally sent from the cyber-victim.

2.1.2.7 Trickery

Trickery is defined by Kowalski et al., [15] as the act of tricking someone to reveal personal information such as who they like the most or their sexual preferences, creating in the cyber-victim a sense of trust, then sharing this information with other people.

2.1.2.8 Exclusion or Ostracism

Exclusion or ostracism according to Willard [29] is the decision about who is accepted in a group and who is not. This happens in the real world as well as in virtual worlds. The author adds that the emotional impact of exclusion may be severe in some youth, as this is considered one of the hardest punishments in society. An example of this cyber-bullying type may be when on a social network a user creates an event for a party invite a certain group of friends leaving others out of this.

2.1.3 Cyber-threats

This very aggressive behaviour allows the perpetrator to make real world threats behind the supposed shelter of the online or virtual world. Willard [29] described cyber-threats as being of two types: direct threats and distressing material. She defined a direct threat as one that shows in a clear and specific way the intention of hurting someone else or themselves, and where there is a current plan to implement or execute it. The plan can contain information as to where and when the event is supposed to take place—such as a date, a specific place or a time. Distressing material is similar to a direct threat; but there is no concrete plan that might hint where this potential event may occur [29]. However, this type of threat also describes the desire to hurt, kill or blow up an individual or a group of people for reasons such as religion and nationality.

Both types of cyber-threat occur mainly in chatrooms, forums, blogs and websites owned by the potential perpetrators, or are sometimes contained in their visible profile status updates. Nonetheless, it is important to remark that not always, fortunately, do these threats come true. The perpetrators may have reacted in a fit of rage triggered by an extreme dislike or disagreement. Even if the threats are not meant to be executed, they should be reported to parents, teachers, relatives, competent authorities, or to a responsible adult and acted upon.

2.1.4 Cyber-stalking

Kowalski et al. [15] describe this online behaviour as when, by the use of electronic communications (such as IM, SMS, posting on social networks and others), the perpetrator stalks their cyber-victim with repetitive harassing and threatening communications. These communications may contain images and/or videos as well as pure text, and may be interpreted as a variation of cyber harassment. Willard [29] defines cyber-stalking as the repeated sending of threats, which are very intimidating for the victim, and

where the communications contain a high level of offensiveness. The author also highlighted that this issue may occasionally include extortion, and is usually linked to relationship problems where photographic material may be involved. An example of this is also outlined by the author, where there has been an interchange of pictures in which one participant has sent nudity pictures. After a problem, or a termination of the relationship, the person possessing the material can start to threaten the ex-boyfriend/girlfriend with sending out the pictures. Or they can actually send the photos to denigrate their ex, and to falsely publish the desire of their victim to meet other people with an interest in having sexual encounters. Cyber-stalking can be considered as somewhere between cyber harassment and cyber-threats [15, 29].

2.2 Consequences

The consequences of the behaviours described above are mainly associated with the non-reporting of these events. However, this is not always true. The damage or impact on a child or teenager has, in many situations, been already done after the first attack. This can be, for instance, the result of an inappropriate photograph published on a social network or sent by MMS through mobile phones. Mishna et al., [19] stated that the prime reasons for not disclosing these problems to a parent or other adult were fear that their computer privileges would be taken away, and also the belief that the adults would not be able to find evidence of the cyber-bullying or identify the aggressor. Consequences are categorised as life threatening, legal, psychological and other.

2.2.1 Life threatening consequences

These are consequences that represent direct attempts on the life of a person. Willard [29] describes some self-destructive or injurious behaviours on cyber-victims such as cutting themselves, using drugs and suicide attempts. In addition to the psychological harm experienced by the victim, disclosing their situation in an online community can lead to victims taking drugs together to feel better or the use of extreme diets causing bulimia and anorexia, as well as recording themselves or broadcasting to an audience that provide support to the person who is undertaking such behaviours. Willard [29] describes even more extreme situations in Japan where the end result is a suicide pact over the Internet. Other sites have taken further advantage of these disturbed online victims to sell online items to accomplish their objectives, such as bracelets and clothing for self-injure.

2.2.2 Legal consequences

Some of the cases of cyber-bullying have gone beyond disciplinary actions taken by the schools and have been transferred to the courts. In the majority of these cases, lawsuits have been raised by parents of the students affected by the decisions of the schools relating to cyber-bullying cases. However, there are also incidents where the schools have taken cases to court for further legal actions. One of these cases, (" Kowalski v. Berkeley County Schools," [15]) is about Sara Kowalski who was a senior at Musselman High School in Berkeley County, West Virginia. She was suspended for five days from school because she created and posted a webpage called S.A.S.H. (allegedly standing for Students Against Sluts Herpes) on MySpace.com in 2005. It was aimed at ridiculing Shay N., another student at the school. Sara invited about 100 students from the same Musselman High School to her webpage. She provided comments, replied with nasty messages on pictures of the target which were uploaded by another student. The school obtained evidence of many students who used the school computers to join and participate both during and after school hours. Kowalski et al., [15] then claimed that, after the event, she got affected by the cold treatment she had received by the students, teachers and administrative staff of the school. It led her to fall into depression and she began to take prescription medicine due to her medical condition. After this, a lawsuit was raised that argued (among other things) the school had violated her free speech rights under the First Amendment by punishing her for speech that had occurred outside the school. Sara went to court arguing that her conduct did take place at home after school, and the webpage she created was subject to full protection under the First Amendment. However, the judges at court threw out her free speech suit as they considered that Sara had “used the Internet to orchestrate a targeted attack on a classmate” [25, para. 14, 15].

Schools do not always win lawsuits against students or their families. In fact, there are many cases where schools have not been favoured by the judges in court because they had gone beyond their school authority. A good example is ("Beussink v. Woodland R-IV School District," [2]), in which Beussink, a student from Woodland School District, created a website which used vulgar language to criticise both school officials and the institution itself. The principal then took measures and suspended the student causing him to fail all of his classes. The student replied by suing the school. The court went in favour of Beussink because the school had not appropriately proved that the website had caused substantial disruption in the educational process.

2.2.3 Psychological and other consequences of online virtual worlds

Kowalski and Fedina [13] reported that children who have been bullied and cyber-bullied present with negative psychological effects such as depression, anxiety and low self-esteem among others. Kowalski and Fedina [13] explained that the perpetrators or cyber-bullies are likely to have suffered the same consequences as their victims. This may be interpreted as a factor that may lead some children and teenagers to become the cause of distress in others. Some cyber-bullies have been victims of online bullying; therefore, once they start to suffer any of the above mentioned psychological effects, they might find relief in making others feel the same.

Didden et al.’s [10] study with 114 students with some intellectual disability sought to identify how children with special needs are being cyber-bullied. Their results showed that children and teenagers with special needs use mobile phones and the Internet to a higher percentage. They are therefore easy targets for cyber-bullies and consequently suffer the negative effects of such problems. The two more common direct effects of being bullyied either by the Internet or by mobile phone services such as SMS or MMS, were self-esteem and depressive feelings. Didden et al., stated that “the more often a student was victimized via the Internet the less self-esteem and the more depressive feelings s/he reported” [10, pp. 149, 150].

ŞAhİN [24] conducted a study stating that there is a correlation between loneliness and cyber-victimisation. This means that victims of cyber-bullying isolate themselves from their peers at school and outside of the campus because they have been victims of some type of cyber-bullying. The author also mentioned this consequence as a problem that may generate further problems such as alcoholism and the use of illicit drugs.

3. A COMPARISON OF CURRENT SOLUTIONS TO CYBER-BULLYING

This section describes some of the current non-technology and technology-based strategies implemented or proposed to minimise or avoid the likelihood and/or impact of the risks identified above.

3.1 Non-technology-based solutions

3.1.1 Policy-based solutions

Rigby [22] contended that people who make decisions about what needs to be done about bullying have to be educated about the topic so as to guarantee a better understanding; therefore, there should be a policy against bullying (p. 236). It was found that "in countries such as Australia, schools are now under increasing pressure to put in place anti-bullying policies and programmes in response to managing the increasing rates of bullying behaviour" [20, p. 230]. Some of these policies also apply to cyber-bullying as it is a new type of traditional bullying. Policies are basically statements created to set out a position against any kind of bullying or cyber-bullying, either by choice or by enforcement of the law. The aim of a policy is to be adopted and applied by teachers, students and all staff working in the institution. A sample policy that outlines how to identify and deal with harassment, intimidation, bullying and cyber-bullying can be found at: http://www.osba.org/Resources/Article/Board_Policy/Sample_policy_JFCF.aspx. Modifying that content to fit our context, the sections of that policy include:

- A definition of cyber-bullying.
- A statement making a strong prohibition of cyber-bullying acts within an educational institution.
- The type of behaviour expected from the students.
- The consequences and action that will be undertaken for people who violate the policy.
- Procedures to report and investigate acts of cyber-bullying.
- A statement that prohibits retaliation.
- Consequences and actions that might be taken on false accusations.
- Statements of how the policy will be published and communicated.
- A definition of roles and responsibilities of who will implement the policy across the institution.

Some countries are establishing and strengthening laws against bullying and cyber-bullying, see for example [6]. In Australia, the government (through the Department of Education, Employment and Workplace Relationships DEEWR) provides two documents as a basis. This gives a guideline on the use of ICT with a better practice guide, and at the same time ensures the safety of students in schools with a framework that applies nationally [9]. However, Campbell [4] found that policies may be different for each school, as they have different needs and requirements that need to be met. Therefore, while it may be useful to consider samples or templates for anti-bullying policies; it might not be appropriate to adopt without change a policy from another school, for instance, without an analysis of what is needed for the specific institution.

3.1.2 Raising awareness

Teachers and parents are not generally aware of cyber-bullying and other types of online issues in educational and non-educational virtual worlds. Campbell [4] suggested that teachers and parents need to be made aware of cyber-bullying and its consequences as they can be repeated and severe. As for teachers, they need adequate training to identify and act in order to prevent and face the issues. As for parents, they need to take care of these issues as their children might have been sending distress messages from their mobile phones or computers. Students within primary, secondary and high schools also need to know about cyber-bullying, cyber-stalking, harassment and any other type of issue from the online virtual worlds. That is why Childnet [5] emphasized the importance of talking about cyber-bullying in schools; clarifying how it differs from traditional bullying; explaining its consequences; detailing methods, strategies and controls to mainly (but not only) prevent it from happening; and finally identifying the sanctions that a cyber-bully may face within the school rules and before the civil authorities.

3.1.3 Taking action

Strategies such as the parents of the bullied child contacting the parents of the cyber-bully, may help to take corrective actions. When the problem is bigger because there have been multiple cyber-bullying attacks or the attacks involve multiple people, a formal request to the school to provide help and a solution on the matter is necessary. Finally, if the cyber-bullying does not stop, the cyber-bully is identified and there is enough evidence, the cyber-victim along with their parents may consider to take the case to court.

3.1.4 Activities to teach students, teachers and parents

Rogers [23] offered in her book a full set of activities to teach students, teachers, parents, and people in general about inappropriate online behaviours, related issues, and the prevention and responses to tackle these problems when they happen (pp. 52–109). The activities are intended to demonstrate scenarios and to make the participants think about the situation and the possible actions to be taken. They also include quizzes where the teachers, for instance, can evaluate how much their students have learned. The objective of the quiz is not to reward but to identify what might not be yet clear for the students.

3.1.5 Promote appropriate use of technology

The Childnet [5] site suggests the promotion of proper uses of technology and e-safety as part of the curriculum in schools so that students can look at the positive things it has to offer such as developing friendships and supporting self-esteem. At the same time, it is vital for teachers to engage with students who can teach one another about new tools, software or social networks that might provide healthy experiences and valuable learning experiences that could utilised in the classroom or at home.

3.1.6 Prohibiting the use of technology devices during the school day

Kowalski and Limber [14] suggested that since most cyber-bullying is done through mobile phones, educational institutions should not allow the use of these devices by students. Policies should explicitly stipulate the prohibition of mobile phones, tablets or similar devices during school time. The consequences for non-compliance should be severe enough to make the rule

effective, along with other controls such as supervision and reporting for school staff and other students.

3.1.7 Supervision

As in real life, the supervision of childrens' online activities may not offer full protection and prevention, but physical supervision may minimise the risk of cyber-bullying. As parents and children tend to see technology in different ways, it is important to establish some physical controls, such as the place where a computer is located within the home, so as to be able to observe children when they are engaging in online activities [4]. Snider [28] suggested not to place computers in children's rooms as parents will not be able to monitor what kind of content they are looking at or what they are posting. A better place is in an open or common area within the house, such as the living room, or near the kitchen or dining table.

3.2 Technology-based solutions

3.2.1 Saving the evidence

Kowalski et al. (2008) suggest that children and parents should save the evidence of a message, posting or image that represents cyber-bullying. To do this it is important that parents or teachers, in the case where the child does not how to do it, have these skills and are able to teach their child how to save, for instance, an IM conversation where there is flaming or other type of cyber-bullying. Also, it is important to keep a soft copy as well as a hard copy of the evidence ideally with the date and time recorded on it. Children must be taught how to print out a conversation or posting found on a webpage or social network in order to prove what and who is disturbing them.

3.2.2 Ignore, block or react

In most cases, the best solution is not to reply to the cyber-bully as replying may encourage further attacks. Better strategies are saving the evidence and ignore or block the cyber-bully from the contact list. As for reacting or replying to the cyber-bully, the cyber-victim should not respond immediately as they can be very affected for the aggressive comments or images published. It is better to wait and consult an adult, such as a teacher or parent, to determine if replying is the best choice. Additionally, the most appropriate answer to this event should be analysed and carefully formulated. Certainly, the cyber-victim must demand from the cyber-bully a stop to this online behaviour.

3.2.3 Requesting to the website or social network to remove offensive material

Another option to stop cyber-bullying is reporting this to the administration of the website where the cyber-victim is being cyber-bullied. An example of this solution is in fact undertaken by social networks such as Facebook, where you can report a picture that you consider offensive or inappropriate for an individual or group of people such as children or people following a specific religion. Facebook allows a button to report this and then the administration of the website can analyse the content and determine whether the content is inappropriate or not and what are the penalties for this action.

3.2.4 Filtering websites

Filtering is a solution that allows defining what websites can be viewed for children and teenagers. This solution is particularly good to block websites with inappropriate content for underage people. However, there are studies (e.g. [12]) which demonstrate that some of the current commercial software for filtering content also blocks some appropriate material. Current commercial software for filtering includes: Net Nanny (http://store.hermanstreet.com/index.php?p=np&page_id=net-nanny-download&ICID=pin-Net%20Nanny%202012-03-20ifr&ofm); Cyber Patrol (http://www.cyberpatrol.com/filter/web-content.asp).; and Websense (http://www.websense.com/content/regional/latam/home.aspx).

3.2.5 Monitoring/Tracking online activities

There are multiple software tools in the market to allow monitoring of activity on a computer to detect if the user is a victim of cyber-bullying or is participating as a cyber-bully or bystander. For example, I am Big Brother (http://www.iambigbrother.com/index.htm) monitors the online activities of the user and includes features such as monitoring multiple IM services, email recording capability, websites viewed, keystroke recording and screen captures. Watch The Tiger (http://www.watchthetiger.com/Index.htm) is a similar tool but also monitors websites such as Facebook, MySpace, eBay, twitter, YouTube, Craigslist and Match.com and allows remote monitoring. This feature is useful for parents to monitor their child from work or any machine. eBLASTER (http://www.spectorsoft.com/products/eBlaster-MobileAndroid/index-h.asp?source=HomePage-hs-ebDroid) allows control of an Android phone by tracking text messages, web history, location through the GPS of the device, voice call log and instant photos taken with the phone's camera to see if the child is taking inappropriate self-photos and sharing them with anyone else. Additionally, there is a feature where the parents may set up a virtual fence around a place, such as their home, a shopping centre, libraries and more, where they can know if their children are in that zone or not. Other products exist for the Blackberry and other phones.

3.2.6 Awareness raising games

A somewhat different product is Privacy Playground which is a game that aims to teach children how to identify marketing strategies to not give away personal information from their parents or themselves, and how to avoid predators [21, para. 2]. The game also contains a guide for teachers that explains the goal of the game, how it may fit in the curriculum, suggestions and expected outcomes among others. Privacy Playground is a game involving three cyber pigs and a little Martian. Children answer questions about the pigs' behaviours and the Martian gives feedback on the answers. One of the important characteristics of this game is the combination of traditional teaching with multimedia.

3.2.7 Mediated/supervised online activities

The Superclubsplus project [27] provides a moderated space for online learning for children from 6 to 12 years old. At this site children can talk to current friends, meet new ones, publish their own material or material from others, and participate in discussions while learning how to use various information and communication technologies. The children are able to participate in quizzes, surveys, conversations with experts or guests and play collaborative games (p. 235). To join the club, children and parents must agree to: avoid spam, protect passwords and other personal information, proper language and behaviour and use of an Emergency Bell if content is found which breaks the rules.

Childnet's Know IT All (KIA) [27] is a UK initiative that includes tailored features, tools and resources for children,

teenagers, parents, carers, teachers and educational institutions such as primary and secondary schools. For example, the site for newly qualified teachers (http://www.childnet-int.org/kia/traineeteachers/) is divided into three parts, where the first one focuses on social networking, the second is called Teachers and Technology and provides a checklist for teachers to see if they are ready to face challenges that technology has. Finally the last subsection includes an E-safety resources matrix and suggests how and when it is appropriate to use the resources in Know IT All.

3.2.8 Artificial Intelligent (AI) Systems

Researchers in the area of virtual companions and intelligent agents have offered some solutions for cyber-bullying. A notable system is FearNot!, an outcome of a European research initiative (http://www.e-circus.org/), where students aged 8-12 participate in a narrative with animated characters to solve situations involving bullying. More recently, van der Zwaan, Dignum, and Jonker [31, 32] proposed the use of a (virtual) dialog agent with whom the child can interact to learn how to use technology to stop or report online perpetrators and their aggressive behaviour. The agent uses a Belief Desire Intention (BDI)-based agent architecture.

The approach follows practice in psychology and counselling and involves five phases as follows:

Phase 1: The agent welcomes the user.

Phase 2: The agent gathers information about the bullying incident.

Phase 3: The agent determines the aim of the conversation.

Phase 4: The agent provides advice to the person using the system.

Phase 5: The dialog is finished.

The aim of the system is to compare the questions asked by the user to internally matched concepts in order to provide appropriate advice and guidance on how to react to cyber-bullying. The system tries to act as a real counsellor without requiring the user's identity to be exposed. The answers provided by the system may encourage the user to report a cyber-bullying incident to a teacher or parent who can take further action on the matter. This potential solution relies on acquiring knowledge from expert psychologists who observe the conversation and intervene, if necessary, when the dialog agent system gives the wrong advice, or provides answers or questions that do not match the conversation initiated by the user. This cycle allows for system improvements until it reaches an acceptable level as specified by several psychologists expert on the topic. At the end of each user conversation, the system attempts to ask questions of the user; for example, "How useful was the advice and the conversation in general?", and "Did you feel you received enough support in to solve the problem?" Future extensions to the database are envisaged so the system can better provide a more natural conversation between the user and the system; acceptable and trustworthy advice; and to teach (where necessary) appropriate responses and use of tools with less involvement of real counsellors.

3.3 A HYBRID SOLUTION

Each application is unique and no-one solution fits all situations. Even within an application, many virtual worlds may exist. However, as a starting point, we recommend that educational virtual worlds should consider the above range of strategies including policy development and enforcement, training and education and tools for detection and intervention and included where possible and appropriate. Further, research in this area should continue so that we see the incorporation of existing techniques, such as van der Zwaan's [32] dialog agent and the narrative intelligence in FearNot! [1], and development of new methods from the fields of data mining and artificial intelligence into the virtual worlds themselves. Currently scripts and production rules are mostly used to provide only limited real intelligence in virtual worlds.

Some of the solutions compared previously are either for preventing, controlling or blocking content and online activities. Just a few of the solutions attempt to interact with the user to teach them what they could be facing in a cyber-bullying event. That is why it is important to have a more complete tool that allows a better approach to the issues in online educational and non-educational virtual worlds. What is suggested here is that monitoring and filtering, for instance, are not sufficiently strong and effective tools to prevent issues such as cyber-bullying. We need to apply something that provides us with a better understanding of what is considered cyber-bullying and when this is happening in real-time.

First of all, we recommend analysing unstructured data to understand better the communications between children and teenagers that take place on sites such as social networks, forums, email communications, and so forth. This activity is called text analytics. It aims to analyse the language used in communications in order to find patterns that may lead us, in this case, to the detection of any sort of cyber-bullying. For text analytics, we suggest using UIMA (http://uima.apache.org/index.html), which stands for "Unstructured Information Management Architecture". It is an open source project by Apache (http://www.apache.org/) that offers frameworks, tools and annotators to programmers in order to simplify the analysis of natural human language into a computer language. UIMA allows development in frameworks such as Java and C++. The latter also supports annotators written in Perl and Python. UIMA is being assessed by the Organization for the Advancement of Structured Information Standards (OASIS) (https://www.oasis-open.org/org) as an official standard. UIMA offers, among its annotators, the Configurable Feature Extractor (CFE), which extracts data from a Common Analysis Structure (CAS). The CFE permits configuration of the rules of the extraction of data through the Feature Extractor Specification Language (FESL) using XML formats. This allows the easy configuration of the information to be extracted to suit the applications of the user. UIMA works just as well for text mining and for analysing information to determine if a cyber-bullying incident is happening. However, this is just how to detect the problem. There is also a need to respond to the safety issues after detection.

Our suggestion is to combine text mining with the reporting of potential threats from victims or bystanders with support for affected cyber-victims. In online educational worlds there is, or should be, constant supervision by teachers and trainers—and sometimes parents as well. In spite of that supervision, things can somehow slip past unnoticed by the text mining application or the supervisors. Thus, children and teenagers, who are members of an educational virtual world, may need a feature enabling them to

communicate or to consult with someone who is experiencing what they (or a friend) are experiencing.

Not all students are very confident talking to an adult about such matters and some adults may not be sympathetic as some think that bullying or cyber-bullying is just a normal phase of growing-up [4]. As a result, students need someone who really understands, cares and guides them while protecting their privacy and confidentiality. It is important to include online help against cyber-bullying in real-time when a student is connected to the online activities within the VW. This help would be something like a button that makes a window come up on the screen presenting the picture of the avatar of the student and also one for the advisor or online helper. This should look familiar to the student, and it must be similar to chat room windows, e.g MSN. In this communication, children might not only report an actual case of cyber-bullying, but also might ask if something can be considered as online bullying or not, as well as asking for direction. The expert advisor will provide help on each case to help the youth act according to the strategies and solutions presented in this paper. Further action will be taken to stop the online perpetrator from continuing to cause distress to other people. The application will filter or block different websites from the one containing the online virtual world unless they have been authorised by the school (it may request this formally by contacting the website). Validation of credential authenticity will be enforced for approval.

Finally, the application could provide videos with illustrations of cases, exposing some of the types of cyber-bullying, the consequences, and how to detect and respond to them. This will be useful for all the actors involved in these issues—such as students, teachers and parents—in order to supply guidance. Along with the technological solution there should be an attempt to provide psychological assistance to the online victims to avoid the consequences of the problems.

4. CONCLUSION

Online virtual worlds offer opportunities for people to have some fun; to build relationships with peers; and to meet new people while learning new knowledge and practicing their ICT skills. As virtual worlds offer many advantages, such as the possibility to access almost any place on Earth through the Internet, this provides a huge educational opportunity that overcomes the limitations of time and place that apply to traditional education. Not only can an online educational virtual world be accessed at different times and locations, the virtual world can create or recreate different time periods and transport the student to anywhere in the universe, or even inside the plant or animal they are studying.

Although online educational and non-educational virtual worlds have their advantages, they also pose various e-safety risks for users. In this paper, we have considered risks related to the behaviour of other users, particularly focusing on cyber-bullying. A number of disparate and partial solutions exist and none of these are specific to virtual worlds. Thus, a key recommendation is that awareness and interest in addressing the safety of children needs to become an agenda item high on the list of researchers and developers of these educational worlds and game engine companies. Regarding online behaviour in general, we suggest a more integrated approach that includes policy, non-technology and technology-based solutions appropriate to aid the cyber-victim and discourage the cyber-bully. This holistic approach should include informing all parties about the rules, issues and consequences of their behaviours when participating in an online educational virtual world; controls to detect and prevent cyber-bullying; and support to those who may be victims. All of this must be packaged in a natural, comprehensive and friendly manner [18]. It must engage students so that they will pass the advice around to help others and change existing culture. Educational Virtual Worlds themselves should be an obvious part of the solution, not an accomplice in the problem.

5. REFERENCES

[1] Aylett, R.S, Paiva, A; and Vala, M. 2007. “FearNot! – an emergent narrative approach to virtual dramas for anti-bullying education”. In: M. Cavazza and S. Donikian (Eds.): *ICVS-VirtStory 2007*, LNCS 4871, 199–202, 2007. Springer.

[2] Beussink v. Woodland R-IV School District (United State District Court, Eastern District of Missouri, Southeastern Division 1998).

[3] Boyd, D. 2012. The Good, the Bad, the Ugly … and the Internet. *Boston Daily*, June 15, 2012. http://www.bostonmagazine.com/news/blog/2012/06/15/roundtable-digital-street/ accessed 6 July 2013.

[4] Campbell, M. A. 2005. “Cyber-bullying: an old problem in a new guise?” *Australian Journal of Guidance and Counselling*, 15(1). doi: 10.1375/ajgc.15.1.68

[5] Childnet. 2007. “Cyber-bullying a whole-school community issue”. 8. Retrieved from *Cyber-bullying Guidance Overview* website: http://www.digizen.org/downloads/cyber-bullyingOverview.pdf

[6] Constitutional Law - First Amendment - Second Circuit Holds that Student's Removal from Class Is Not First Amendment Retaliation Where Motivation Is Protective. - Cox v. Warwick Valley Central School District, 654 F.3d 267 (2d Cir. 2011). (2012). [Article]. *Harvard Law Review*, 125(4), 1096-1103.

[7] Crookall, D., Oxford, R. and Saunders, D. 1987. “Towards a Reconceptualization of Simulation: From Representation to Reality”. *Simulation/Games for Learning*, 17(4):147-71.

[8] Crystal, D. 2006. *Language and the Internet*: Cambridge University Press.

[9] Student Learning and Support Services Taskforce of the Ministerial Council on Education, Employment, Training and Youth Affairs. (DEEWR) 2003. *National Safe Schools Framework* Retrieved May 16, 2012, from http://www.cybersmart.gov.au/Schools/Cybersafety%20policies%20and%20procedures/National%20or%20state%20and%20territory%20policies/National%20cybersafety%20policies.aspx#BetterPracticeGuide:ICTinschools

[10] Didden, Robert, Ron H. J. Scholte, Hubert Korzilius, Jan M. H. de Moor, Anne Vermeulen, Mark O’Reilly, Lancioni, G. E. 2009. “Cyber-bullying among students with intellectual and developmental disability in special education settings”. *Developmental Neurorehabilitation*, 12(3), 146-151. doi: 10.1080/17518420902971356

[11] Garner, B. A. 2004. *Black's Law Dictionary*.

[12] Hunter, C. D. 2000. “Internet filter effectiveness (student paper panel): testing over and underinclusive blocking decisions of four popular filters”. Paper presented at the

Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions, Toronto, Ontario, Canada.

[13] Kowalski, R. M., & Fedina, C. 2011. "Cyber-bullying in ADHD and Asperger Syndrome populations". *Research in Autism Spectrum Disorders*, 5(3), 1201-1208. doi: 10.1016/j.rasd.2011.01.007

[14] Kowalski RM, Limber SP. Cyber bullying among middle school students. J Adolesc Health 2007;41(Suppl):S22–S30.

[15] Kowalski, R. M., Limber, S. P., & Agatston, P. W. 2008. *Cyber-bullying Bullying in the Digital Age* (1st ed. ed.): Blackwell Publishing.

[16] Kowalski v. Berkeley County Schools (United States Court of Appeals, Fourth Circuit II 2011).

[17] McQuade, S. C., Colt, J. P., & Meyer, N. B. B. 2009. "Cyber-bullying: protecting kids and adults from online bullies" Retrieved from http://lib.myilibrary.com/Open.aspx?id=234119&loc=&srch=undefined&src=0

[18] Minocha, S., & Reeves, A. 2010. "Interaction Design and Usability of Learning Spaces in 3D Multi-user Virtual Worlds", *Human Work Interaction Design: Usability in Social, Cultural and Organizational Contexts IFIP Advances in Information and Communication Technology*, 2010, Volume 316/2010, 157-167.

[19] Mishna, F., Michael Saini, & Steven Solomon. 2009. "Ongoing and online: Children and youth's perceptions of cyber-bullying". *Children and Youth Services Review*, 31(12), 1222-1228. doi: 10.1016/j.childyouth.2009.05.004

[20] Ng, E. 2010. *Breaking the Silence*: Armour Pub.

[21] Network, M. A. 2010. Privacy Playground Retrieved May 16, 2012, from http://www.media-awareness.ca/english/games/privacy_playground/

[22] Rigby, K. 2002. *New Perspectives on Bullying* (illustrated ed.). United Kingdom: Jessica Kingsley Publishers.

[23] Rogers, V. 2010. *Cyber-bulling, Activities to Help Children and Teens to Stay Safe in a Texting, Twittering, Social Networking World* (pp. 128).

[24] ŞAhİN, M. (2012). The relationship between the cyber-bullying/cybervictmization and loneliness among adolescents. *Children and Youth Services Review*, 34(4), 834-837. doi: 10.1016/j.childyouth.2012.01.010

[25] Savage, D. G. 2012, January 15, 2012 11:07 p.m. Supreme Court to consider cyber-bullying cases Retrieved 04/06/2012, 2012, from http://poststar.com/news/local/supreme-court-to-consider-cyber-bullying-cases/article_1ca81a24-3ff8-11e1-bc9a-0019bb2963f4.html

[26] Schrock, Andrew and Boyd, Danah,2011. Problematic Youth Interaction Online: Solicitation, Harassment, and Cyberbullying. In *Computer - Mediated Communication in Personal Relationships* (Eds. Kevin B. Wright & Lynn M. Webb). New York: Peter Lang.

[27] Shariff, S., & Churchill, A. H. 2010. Truths and Myths of Cyber-Bullying: *International Perspectives on Stakeholder Responsibility and Children's Safety*: Peter Lang.

[28] Snider, M. 2004. "How to Cyber-bully-Proof Your Kids". Retrieved 8/7/12 from http://www.macleans.ca/science/technology/article.jsp?content=20040524_81184_81184.

[29] Willard, N. E. 2007. *Cyber-Bullying and Cyber-Threats responding to the challenge of online social aggression, threats, and distress.* Research Press.

[30] Yun-yin Huang, & Chou, C. 2010. "An analysis of multiple factors of cyber-bullying among junior high school students in Taiwan". *Computers in Human Behavior*, 26(6), 1581-1590. doi: 10.1016/j.chb.2010.06.005

[31] Zwaan, J. van der, Dignum, V., & Jonker, C.M. 2012a. "A BDI dialogue agent for social support: specification and evaluation method". In *Proc. of the International Workshop on Emotional and Empathic Agents (EEA 2012).*

[32] Zwaan, J. van der, Dignum, V., & Jonker, C.M. 2012b. "On Technology against Cyber-bullying". Technical Report. Delft University of Technology.