Fachhochschule
Polizei Brandenburg

ORANIENBURGER SCHRIFTEN

Articles of the University of Applied Science of the Brandenburg Police

Special Edition 2013

FROM THE CONTENT

Table of Contents

Editorial

Ladies and Gentlemen,

For a president of a higher education establishment of the police it is always a special joy to be presented with a scientific publication from your own institution. Since the year 2007, the University of Applied Science of the Brandenburg Police (Fachhochschule der Polizei des Landes Brandenburg) has been regularly publishing a German-language research booklet called Oranienburger Schriften. The publication is devoted to phenomena relevant to police work within the context of the booklet's particular focal points.

Every so often a topic is raised that is of greater and more international significance than can be reflected in a German-language publication. We believe that, from a research perspective, the present edition deals with just such a topic, and one that so far is largely unknown.

With support from our interior minister Dr Dietmar Woidke, we have decided for the first time to publish an edition in English in order to bring the findings about the victimisation of minors by sex offenders in the virtual worlds to the attention of the widest possible audience.

I hope that some readers, having read this publication, will engage in scientific exchange with us. I would be delighted.

Yours,

Rainer Grieger
President of the University of Applied Science of the Brandenburg Police

Preface

of the Interior Minister of the State of Brandenburg

Ladies and Gentlemen,

On 19 September 2012 the interior ministry on behalf of the State of Brandenburg organised a conference in Brussels on the risks of virtual worlds. The conference was designed to make the European Commission, the European Parliament and other bodies interested in this topic aware of the risks inherent in the use of online games (which are also used by sex offenders) for children and young people. I thought that it was expedient to hold this conference because the very essence of the task of policy-makers is to improve things in the face of blatant wrongdoings. The many positive national and international reactions and the feedback from the media we received confirmed my belief that such an event was necessary and beneficial.

I was all the more surprised that until now almost nobody has seriously looked into the dangers inherent in the use of virtual worlds by sex offenders and the accompanying lack of mechanisms in place that protect children and young people. Although for many children and young people online games are a media reality and are for some, depending on their age, more popular than chat rooms, the risks have so far not been examined in depth. We are not talking about whether these games have violent or pornographic contents, we are talking about who plays, interacts and communicates in such worlds, which is something that needs to be looked into. It is therefore necessary to critically review the safety mechanisms of such games that are currently used and place them in an international (European) context. Here, the operators as well as the responsible child and youth protection authorities must be called to task and asked to reconsider their safety precautions. In addition to these technical and policy measures, users and especially their parents have to be made aware of these risks. I believe that this is necessary to allow parents and their children to discuss the responsible use of the internet.

This publication can, on the one hand, contribute to making the internet as safe as possible for minors to use and, on the other, bring about new ideas for security agencies with regard to law enforcement as well as prevention. I hope that this special edition of Oranienburger Schriften will help people become more aware of these risks.

Yours,

Dietmar Woidke

Dr Dietmar Woidke
Interior Minister
of the State of Brandenburg

Sex offenders in the virtual worlds

Thomas-Gabriel Rüdiger, M.A.

Abstract

Virtual worlds and online games in particular are played by more and more people every year. In its heyday, the well-known online game World of Warcraft alone attracted 12 million people. In Germany, 16 million people are already playing online games. Virtual worlds bring together people of all ages and gender in playful interaction without them ever knowing exactly who the other players are. A fraction of them use this anonymity and intimate interactive experience to initiate sexual contact with minors. There are two main types of offenders. The blackmailer type who acts openly and the good-friend type who acts in a conspiratorial way. Both types of offenders take advantage of the specifics of virtual worlds for instance to entice children to commit sexual acts in return for virtual goods. This practice is facilitated by youth protection laws that cannot yet accommodate the interactive and communicative risks associated with such games and by a lack of knowledge of parents and the social institutions about this medium.

"In online games where you can get some bonus points. When a child meets someone unknown in such game and that person offers him or her buying those points if the child sends him some naked photos."

1. Introduction

"In online games where you can get some bonus points. When a child meets someone unknown in such game and that person offers him or her buying those points if the child sends him some naked photos."

The opening quote of this article is by a 12-year-old boy from the Czech Republic and comes from an official report from the research project "EU Kids Online" (Livingstone et.al, 2011-1).

In only two sentences, the boy vividly describes his experiences with the phenomenon of what is called cyber grooming when playing online games. These are not the only descriptions of sex offenders in virtual worlds from official EU reports. In the same report, an 11-year-old boy from Belgium reports: *"I was playing a game with [my friend] online and we bumped into something like sex and it was all over the screen"* (ibid.). In a follow-up report from the same research project a 15-year-old girl from Turkey describes her experiences as follows: *"When I am playing games with my older sister on the internet, naked people pop up and it is very bad"* (Livingstone et. al, 2011-2).

Although these depictions vividly expose the risks of sexual harassment in virtual worlds for minors, so far, this phenomenon has not yet attracted widespread political or scientific debate. The present article will therefore address this particular online practice of sex offenders and expose the problems of the virtual worlds as a platform for sex offences. In a first step we will describe the social, economic and technological mechanisms of the virtual worlds necessary to understand the issue as a whole, and link these findings with basic insights into cyber grooming processes in a next step. In a final step, based on this starting position, we will analyse and identify enabling and limiting factors and formulate initial proposals for better online protection of children and young people.

2. Virtual worlds

Worldwide, more than two billion people use the internet and couldn't imagine life without it (Pingdom, 2012). The internet permeates almost every aspect of human activity and interaction. People use the opportunities opened up by the internet in many different ways – from online shopping and virtual meetings to doing background research. A crucial economic and cultural factor is how it shapes people's recreational habits, which is being more and more affected by the use of social media. This not only includes the classic social networks such as Facebook, Xing and Google Plus and video platforms like YouTube and MyVideo, but also so-called virtual worlds.

Virtual worlds are programmed fantasy worlds where a large number of people can interact with each other (e.g. communicate, act, play, fight, sing, dance). To visualise these interactions, in most virtual worlds users play with interactively controllable images of themselves – the so-called avatars[1]. As yet, no scholarly definition of 'virtual worlds' has become established. However, it is commonly associated with the features immersion (an emotional immersion into the environment, generally through the avatar), persistence (the development of the world independent of whether the user is online or not) and consistency (all users are able to perceive the same things) (Meyfarth, 2007). What's truly extraordinary about virtual worlds is that millions of people worldwide interact and communicate with and through their avatars, which generates myriads of social processes every day. Like any other interaction between people, these processes can have positive as well as negative consequences.

What's truly extraordinary about virtual worlds is that millions of people worldwide interact and communicate with and through their avatars, which generates myriads of social processes every day.

Researchers currently divide virtual worlds into metaverses and online games. Metaverses, which are also called life simulations, do not (wish to) prescribe a specific goal to the users. Rather (like with the classic social networks) social interaction is the focus of the experience. One of the most well-known metaverses is Second Life, which caused a veritable online hype especially in 2007. The goal of Second Life is to virtually recreate life in all its complexity (Krebs & Rüdiger, 2010). In 2012, Linden Labs, the operator of Second Life, announced that every day 80,000 people are online and a total of 32 million avatars (or 'residents') have been created (Dwell, 2012). A special feature of Second Life is that users can create their own content (also called 'user content') and integrate, use and even sell it in this virtual world. One of the consequences of this was that serious violent and sexual acts (for example the so-called Dolcett plays) have been programmed into Second Life by some users and made them experienceable for other users (Rüdiger, 2013-1). In addition to Second Life there are several other versions such as There, Secret City and the Facebook-based Cloud Party. 2D and 3D communities such as Habbo Hotel, Smeet, Freggers and Club Coee may also be counted among the metaverses. The aim of these worlds is to make the social networks more experienceable especially for minors using interactive graphic interfaces and avatars.

Online games on the other hand place a clear focus on the playful element. This means that users are given goals and tasks (in whatever form), which they have to perform or reach alone or together with others. To make these games attractive to as large a target group as possible, there are different game concepts and design forms. The best known of the online games are probably the massively multiplayer online role-playing games (MMORPGS). In these games millions of people play together in a medieval-looking fantasy world[2] using their avatars that can be visually adjusted. Blizzard, the operator of the most commercially and probably critically successful MMORPG World of Warcraft, announced at a press conference on 7 October 2010 that the game now has more than twelve million paying users (Blizzard, 2010). In connection with the triumph of mobile devices with internet access, so-called browser and social games have become established on the market. These

[1] The term "avatar"comes from Sanskrit meaning "a deity on earth" (Erenli 2008, p.4).

[2] MMORPGs can have a number of settings, from science fiction and horror to agent scenarios.

are usually strategy games where users have to build and look after a country, a city or something similar, and there are also version where the development of the avatar is the main focus. Social games are games that are either directly integrated into a social network (a well-known example is Farmville, which is integrated into Facebook) or where the concept is based on trying to encourage as many of your own contacts in the social networks as possible to play. Almost 15 percent of Facebook's multi-billion dollar turnover is said to be generated by Zynga games, which are based on this concept (Tagesspiegel, 2012). Another important genre are online-based multiplayer parts of computer and video games. There is currently almost not a single classic disk-based game that does not give users the option of playing with or against other players online. For many players, this aspect is now the reason they purchase the game. Here, so-called first-person shooters (such as Call of Duty and Battlefield Reihe) are particularly popular, as are sports games (such as FIFA and PES football games).

The impact that such virtual worlds currently have on the media landscape and on media use is best reflected in the latest user numbers. In Germany alone, around 24 million people play computer games (Bitkom, 2012). Around one in five Germans (that is a total of approx. 16.5 million people) play online (BIU, 2012). What's more, according to a representative study for Germany, in 2012 66 percent of 6 to 9-year-olds and 75 percent of 10 to 13-year-olds spent their spare time playing online games (KidsVA, 2012). According to the KIM study 2010 on the other hand, in Germany only 15 percent of 6 to 9-year-olds and 50 percent of 10 to 13-year olds regularly use chat rooms (KIM, 2010). It is likely that with current technical developments the number of active computer game players will continue to grow in the coming years. The growing popularity of smartphones and pads (which are just mobile mini computers) in particular are catalysts for this trend. Already in the first quarter of 2012 one in three mobile phones in Germany was a smartphone (Pakalski, 2012). Smartphones do not just have adults as their target group, as much as 63 percent of children now own their own mobile, one in five of which is an internet-enabled smartphone (YouGov, 2012). This figure does not include the number of minors who use the smartphones or tablets of friends and relatives for example on the bus or during family celebrations to pass the time. The current popularity of smartphones goes hand in hand with increasingly cheaper internet flat rate tariffs. Operators of virtual worlds are recognising this trend and increasingly focus on products that allow users to play games together on mobile devices. This in turn particularly attracts casual gamers – as well as children (Bitkom, 2012-1). According to one study, in 2012 73 percent of children in Germany played games on their mobile or smartphone (ibid.). Another European study found that the majority of today's generation of children had their first internet experience through the medium of online games (Livingstone et.al, 2011-2, S. 14).

What's more, according to a representative study for Germany, in 2012 66 percent of 6 to 9-year-olds and 75 percent of 10 to 13-year-olds spent their spare time playing online games (KidsVA, 2012).

3. Economic considerations

The makers of virtual worlds have one main goal: to sell as many of their products as possible. Traditionally, operators in the past have relied on a financing concept that generates revenue through acquisition costs and a fixed monthly fee. This basic fee in particular promised huge profits for successful games. In 2010, Blizzard for instance generated almost one billion US dollars with its roughly 12-euro monthly fee for World of Warcraft (PCGames, 2012). The idea behind the monthly fee and the pay-to-play (P2P) financing model is that the user regularly pays for playing the game, providing the operator with a predictable income. Sometimes users pay additional money for virtual items or additional services.

The sale of virtual items in particular has developed into a highly profitable financing model over the past few years. In advertising, *In fact, market analysts believe that by 2015 almost 12 billion US dollars of turnover will be generated with virtual game items (InStat, 2011).*

the model is often described as "free", which is where the term "free-to-play (F2P)" comes from. In this model, the playing the game is indeed free of charge for the user. Revenue is generated through the sale of items (such as swords, furniture, pets, armour) or special additional services. The games are designed in such a way that the player will be able to play the game and gain a sense of achievement very quickly, thus being encouraged to carry on playing. Specifically, an F2P strategic browser game could be structured in such a way that the user has to build a medieval town and an army. At the beginning building houses and increasing the number of inhabitants only takes a few seconds, and as you play on this can take several days. As a countermove, players are given the option of speeding up construction time by paying money. The money is described using such mystical and customer-friendly terms as "magical coins" or "precious crystals". But the user has to first purchase this virtual currency with real money. Usually this can be done with payment methods such as credit card, Paypal or Paysafecard. Many players also use an over-the-phone payment method. The user determines how much money he spends on the virtual currency; some games temporarily limit the amount and the frequency with which you can do that. Then the user is assigned a personal multi-digit number and has to call a hotline (which usually incurs a charge) or send an SMS to such a hotline. Once the number has been provided, the money will be charged to the account holder's telephone bill[3]. Buying items in F2P-MMORPG works in a similar way. With MMORPGs, users become stronger by beating opponents (usually monsters) and solving challenges; as a reward, so to speak, they are given items of equipment that make them even stronger. Usually, which items are left behind (or dropped) by the defeated monsters is based on chance. At the beginning of the game, during the achievement phase, items are found more frequently and have a value that is appropriate to the game level. However, the longer a player plays the game the less frequently strong and powerful items are dropped. Items such as weapons and armour, if they are worn, can be seen on the avatar. A player's status, success and especially the amount of time spent playing with others is displayed by wearing the relevant items. The longer a player spends playing the game, the longer he may take to achieve success. Some players (as already noted) are therefore prepared to buy or swap such advantages to avoid spending a lot of time playing the game to get them. In many virtual worlds users have the option of trading and swapping items and virtual currency with others and even of giving them away.

The industry believes that currently on average only one in ten users is prepared to spend money on such virtual goods. Among the new generation of players (18 to 29-year olds) one in five has spent money on virtual game content (Bitkom, 2012-2). In Germany in the year 2011 alone, a total turnover of 233 million euros was generated by trading items and buying virtual additional services (BIU, 2011). In fact, market analysts believe that by 2015 almost 12 billion US dollars of turnover will be generated with virtual game items (InStat, 2011). The relatively small number of people prepared to pay relative to absolute numbers of users shows that game operators must have an interest in making accessing the game as attractive and easy as possible in order to attract as many users as possible to it. Registering with virtual worlds is therefore rather easy. Usually, users enter an email address, as username, a password and occasionally their age. The registering person or their age generally gets verified through a simple

[3] Every so often, with this payment model minors, without their parents' knowledge or permission, can run up phone bills to 10,000 euros per month for virtual goods. The majority of parents are sentenced by the courts to pay their bill, pointing out that they should have blocked the use of premium rate numbers. An exception was a court decision taken in Saarbrücken, where the judge criticised, amongst other things, a lack of protection of children and minors in online games (LG Saarbrücken, 2011).

verification email, if at all. Such a simple and, from a child and youth protection point of view, unsatisfactory registration process without any barriers allows users to start a game very quickly. For these same reasons it may also be in the interest of operators not to come into conflict with regulations governing the protection of children and minors and thus obtaining a low age rating. This is one of the reasons why many of today's online games do not contain pornographic or violent content and instead focus on colourful games graphics that are suitable for children. Viewed critically, such graphics combined with the game being allegedly "free" can lower parents' awareness for the inherent risks of the internet and also for the existence of the corresponding payment models.

Independent of which payment model is used by the virtual world, at some point the user (especially if they are minors) may no longer have enough money to pursue their passion for the game the way they want to. In recent years it has been increasingly debated worldwide, including in Germany, whether the excessive playing of online games can lead to addiction or dependence amongst users. A number of relevant studies have been carried out, which ultimately differ only with regard to the number of people affected, and not the existence of the phenomenon itself (Pfeiffer et al., 2009; Fritz et al., 2011; Rumpf et al., 2011).

A preliminary conclusion is that virtual worlds are highly attractive to many people, especially minors, because they give users opportunities for interaction and communication. Conversely, the identity and age of the people who register is not verified in most cases.

4. Cyber grooming

Traditionally, minors are an important target group for virtual worlds. One of the indications for this is that a great many games are at least visually targeted directly to this group. The metaverse Habbo Hotel is one example; according to the company's own information it has approx. 14 million active users and approx. 250 million people access it worldwide (Sulake, 2012). 90 percent of users are said to be between the ages of 13 and 19 (ibid.). Given that no effective age verification system is in place, these figures are in principle questionable because people's actual age is not established during the registration process. Although anonymisation in the virtual world is used in a positive way by many people (by allowing them to become a different gender or have different character and create a virtual identity) (Cole; Griffith 2007), there are people who deliberately obscure their age and gender to gain the trust of minors with this alleged identity. The aim of such behaviour is to instigate sexual interaction with minors – so-called cyber grooming (Rüdiger, 2012).

The term 'grooming' was defined by Dutch psychologist Ruud Bullens in 1995 as the planning phase that precedes a sexual assault on a child by an adult (Bullens, 1995, p.55). Clearly, Bullens' discussion did not refer to the internet as the platform of this phenomenon, so that the component 'cyber' did not have relevance for him. The term 'cyber grooming' was coined by combing the two words. Based on Bullens' definition of 'grooming', we might define cyber grooming as "the initiating of sexual acts with minors by taking advantage of the anonymity and the communication options available on the internet as a preparation stage for sexual interaction". In a British context the name for the perpetrator has become established as "(cyber) groomer" (ibid, S. 92) and in US English as "online predator" (Finkelhor et. al., 2008). Finkelhor analysed 6,594 registered rapes in the USA and concluded that as early as 2008 seven percent of these were initiated online (ibid.). Studies carried out to date almost entirely discuss actions in typical chat forums without taking into account any graphic environments and interactions with an avatar or a game environment (Choo, 2009; Finkelhor et. al., 2008; Ybarra; Mitchell,

Based on Bullens' definition of 'grooming', we might define cyber grooming as "the initiating of sexual acts with minors by taking advantage of the anonymity and the communication options available on the internet as a preparation stage for sexual interaction".

2005). In the German-speaking region, it was Katzer in 2007 who carried out the first study on the victimisation of young people in chat rooms through sexual violence (Katzer, 2007). Katzer came to the conclusion that sexual victimisation of minors (girls in particular) takes place even more frequently than in the psychologically real world because of the anonymity granted there (ibid, p. 79). He also noted that adolescent girls in particular tend to give themselves sexually explicit nicknames in chat forums, which in turn increases the likelihood of them being victimised. An analysis of this survey showed that as much as 48 percent of girls under the age of 14 have experienced unwanted sexual communication online, 26 percent stated that they have been asked about sexual experiences unprompted, 24 percent were asked to actively describe such experiences, and eleven percent said that they have been invited to meet someone in person at least once (ibid, p. 88).

An analysis of this survey showed that as much as 48 percent of girls under the age of 14 have experienced unwanted sexual communication online, 26 percent stated that they have been asked about sexual experiences unprompted, 24 percent were asked to actively describe such experiences, and eleven percent said that they have been invited to meet someone in person at least once (ibid, p. 88).

Given the growing number of people with access to the internet, which among minors in Germany is nearly one hundred percent, it seems likely that the victimisation rate worldwide has increased rather than dropped.

5. Offender typologies

Two main typologies of cyber groomers have been identified to date. The "blackmailer" or "direct" type who acts relatively openly and the more conspiratorial "good friend" type. In this articles both offender typologies will be described mainly using the German-language Habbo Hotel as an example, but also a number of other virtual worlds.

To help understand the actions of both offender typologies, the interaction and communication in virtual worlds in general will first be explained.

To register with the Habbo Hotel you need to enter a username, create a password and enter an email address. In the German-language Habbo Hotel the validity of the email address is not checked, for example by sending out verification emails. Once the user has registered he will be in a virtual hotel room. Habbo Hotel makes money by selling virtual furniture, clothing and pets to its users. The sale of pets (such as ponies, cats and rabbits) is particularly targeted at minors. Not only pets are paid for using so-called Habbo talers (the virtual currency in the Habbo Hotel), pet food also has to be bought regularly. In the game shop it says *"Pets need food, water and rewards. Here you can find everything you need to look after your pets"*. In Habbo Hotel users also have the option of swapping items or giving them away.

Users in Habbo (and this is similar in most virtual worlds) come into contact with each other in two main ways. In the lobby and themed rooms many users and their avatars get together, where they can write to each other using the chat function, which is visible to all. If two users want to communicate with each other directly and without anyone else reading along, they can use an internal chat and messaging function. To do this, users have to connect with each other first by sending and accepting a friendship request (FR). Users can also retreat to the individual private hotel rooms, where others users cannot see what they are talking about. During the communication the avatars can interact with each other, such as dance with each other, lie in the same bed together or sit at the same table. Sex offenders have a great number of verbal and non-verbal opportunities for contact with potential underage victims available to them.

The blackmailer type

The blackmailer type usually acts in a direct and open way when initiating sexual contacts. His main intention is to engage in sexually related contact with a minor. As soon as he has achieved this, he can use this contact to encourage the victim to create or have someone else create more and more media (such as photos and videos) depicting the victim. If the victim no longer wishes to participate or terminates the contact, the offender responds in various ways. In the best case, he will also cease contact with that user. In the worst case (as in the example of Amanda Todd) he will threaten to send the photos or videos to parents or friends or to publish them on the net if the victim does not permit further sexual interaction.

In order to initiate such contact with minors in the first place, offenders use two main methods of initiation. The most obvious one is when the offender specifically searches for victims using the public chat feature. This may look as follows: *“Which girl with Skype, MSN or ICQ fancies using the cam,?“* (Rüdiger, 2012). Other inquiries at Habbo Hotel included: *“who wants to see a morning wood”* or *“who wants to see what I have below?”*. Even though such questions, from an adult’s perspective, can be viewed as obviously problematic, it cannot be ruled out that adolescents respond to such question purely out of curiosity.

Another tactic is to offer minors items and virtual currency in return for sending pictures or using the web cam. Again and again you encounter inquiries in the public hotel rooms of Habbo Hotel such as *“which girl with a webcam wants to earn 70 – 100 talers (approx. 12 euros), please FR”* (ibid.). Other cases are known where, for example, underage victims in World of Warcraft were paid with virtual gold for taking and sending naked pictures of themselves. In one such case a 28-year-old Danish man paid boys between the ages of 12 and 16 with gold for World of Warcraft for sending naked photos and videos depicting the boys masturbating (Chalk, 2010).

In one such case a 28-year-old Danish man paid boys between the ages of 12 and 16 with gold for World of Warcraft for sending naked photos and videos depicting the boys masturbating (Chalk, 2010).

In order to make sure that he actually receives these images and photos and perhaps even get the victim to participate in a live video chat, the blackmailer type generally tries to transfer the communication quickly to an instant messenger such as ICQ and especially Skype. For instance, in order to get into contact with a minor over Skype, all the offender needs to know is the person’s username. The offender will try to find out this username in Habbo Hotel or another online game or chat portal, which is why such questions as *“which girl with Skype […]”* are common. As soon as the victim has disclosed their Skype name, the offender ads it to his own contact list. Here he benefits from the fact that Skype is set up such that an incoming video call automatically shows the caller live – whether the user wants to accept the call or even whether a web cam is connected or not. If a video stream is set up, the offender can record the entire video or save individual screenshots. Skype also offers the option of data transfer via the integrated chat feature, which allows images and videos to be exchanged relatively easily. This means that the victim could, for instance, quite easily send naked photos taken by the webcam to the offender. If a victim does take videos and photos of a pornographic character, then ultimately this is tantamount to creating and being in possession of criminal child and youth pornography.

The tragic example of 15-year-old Canadian girl Amanda Todd shows how the blackmailer type then proceeds. At the age of 12 Amanda Todd was encouraged by men to bear her breasts in front of a webcam. As already described, screenshots were then taken of Amanda. Subsequently, one of the men contacted Amanda through Facebook and demanded more naked photos from her and, in case she refused, threatened to publish the photos already in his possession online. Amanda refused further sexual contact with the offender, whereupon the offender set up a fake Facebook account, used these photos as profile pictures and then sent out a group email. Amanda then became the victim of peer bullying and suffered from constant cyber bullying attacks. It is likely that these constant attacks led her to take her own life on 10 October 2012 (Shaw, 2012). The example of Amanda makes it very clear how these offenders operate. When looking for victims, it benefits the blackmailer type that in virtual worlds minors give their avatars names that allow you to guess their age. Numbers after the name often indicate an age, for example “Sunflower12” (12 years of age) or “Sunflower99” (born in 1999 , therefore 12 years of age). Names such as “Checker15” (boy, 15 years) can also give information about gender. Sometimes the nicknames already convey a sexual message such as “hu.ge.co.ck19“ or “sexybitch13” (Breichler et.al, 2009, p.9). Many users tend to give their avatars their own gender, which makes it easier for the offender (because of the avatar’s gender and the username) to select his victims.

> *“Hi srry I will sound a bit silly but I really need your help it’s embarrassingmy hand’s really hurting”? what do you mean? I am wanking off and can’t finish it how embarrassing ;(((How should I help? Can’t you watch me? And how? Well via the xxcamxx ?“*

Sometimes offenders start their communication by directly asking for cybersex (CS). Cybersex stands for a form of interactive erotic written communication, the intensity of which is most comparable to verbal erotic contact, such as telephone sex. Users write about their sexual phantasies to each other or respond to the comments of the other person. This results in intimate communication that is often pornographic in character. Such conversations can start quite innocently. In MMORPG, for example, initial contact may consist in referring to the design of the (usually female) avatar. Depending on the success of this initiation phase, and also on the motivations of the offender, the conversation is continued and can then be transferred to the IRCs. The offenders rely on minors being more likely to open up to sexual conversations simply out of curiosity and because no videos or pictures get transmitted.

A participant-observation study (using a childish cover in online games and children’s chatrooms) found evidence that offenders act this way. Such a study was carried out in the German-language Habbo Hotel, for example, on 28 February 2013 between 1 and 4 p.m. The public chatrooms most highly frequented at that time were visited for the purposes of the observation. A total of 25 relevant communication attempts were identified (Rüdiger, 2013-2). 15 of these attempts were specific requests for sexual acts (such as cam sex) or people asking for Skype or ICQ. For example, this category included the following statements made by various avatars: *“Which girl fancies exchanging pictures? Send FR ☺”, “Looking for a boy with a long one for Real Meeting PSL[please] contact me”, “looking for percverse girl with skyxpe”*[4] . In addition, there were five direct attempts to initiate contact with the undercover avatar, two of which will be presented here. The offender in this case passively encouraged the potential victim, rather than actively. In the first one, the following request was made in the public chat channel: *“You are female and want to earn 140 talers [approx. 20 euros]? ← offer FR ←…☺”*. Subsequently the same user wrote to the undercover avatar: *“Hi how xold?* 13, but almost 14! *Do you have a xcam?* You mean skip? *And a xwebxcam on the notebook.* What should I do? *You can earn 140 talers by showing me something over the xcam!* What? *Xmore of you.* Have to wait, mum’s here. *How long for* (communication is terminated)”. In the second case the undercover avatar was again contacted by a user: *“Hi srry I will sound a bit silly but I really need your help it’s embarrassingmy hand’s really hurting”*? what do you mean? *I am wanking off and can’t finish it how embarrassing ;(((How should I help? Can’t you watch me?* And how? Well via the xxcamxx ? how old? 17 and will you help me? But I am younger! How old are you? 13. Doesn’t matter please help me let’s use the webcamxx please”. The other three contact initiations went along similar lines. Within three hours at least five sexual victimisations of minors could have taken place in the worst case (ibid.).

In a second round on 2 March 2013 between noon and 12:40 p.m. in a lobby of Habbo Hotel, a total of 26 such comments from 22 avatars were identified. These

[4] The deliberate misspellings are (as already mentioned) designed to avoid the word filtering in Habbo Hotel. The article provides a literal rendition.

were divided into 18 open inquiries such as: *"I want xcam sexx ;☺","Which girl wants to watch me ☺ ?:) fr ☺"* or *"Which girl is xperverted? Send FR"*. Six more comments were of a sexual nature and repeats and two were direct requests to the undercover avatar regarding continuing the conversation on skype (ibid)[5]. What attracted attention during the participant-observation was the fact that some users directly asked others to swap images using the popular smartphone messenger WhatsApp, for example: *"let'sgox on skyipe or xwhattsapp and send xpictures or habbo sxx?"*. For the offender continuing communication on the WhatsApp would have several advantages. First, to communicate with this programme, users have to swap mobile numbers, which would allow other forms of harassment and ways of approaching the victim, and second, via WhatsApp media files, and therefore also images that people have created of themselves, can be exchanged easily.

Many international examples show how the blackmailer type operates. In the year 2011, a 19-year-old man from New York was arrested who groomed and sexually abused a 13-year-old boy via the games console Xbox (Fahey, 2011). The offender called his gamer tag (user's nickname, profile and success in the game so far visible to other players), which can be seen by all players, "homosexual furry". The offender here took advantage of the fact that in millions of living rooms and children's rooms worldwide you find Xboxes and Playstations and these are used to play online by a great many people. The Xbox as well as Playstation both sold 70 million game consoles each in 2012 (Leschni, 2012). Both systems also offer the option of contacting fellow players and, by sending/accepting a friendship request, getting closer to each other. The systems also offer the opportunity to install to a Playstation Eye or the Xbox Kinect to allow live video broadcasts. Habbo Hotel is also versatile as an initiation platform. In September 2012, a 25-year-old former police officer in England was sentenced to three and a half years in prison. The offender used Habbo Hotel to specifically talk to underage boys and get them to watch sexual acts on their webcam via Skype or MSN (Phagura, 2012).

There are countless versions of this type of offender. Some pretend to be employees of a youth magazine or a model agency to ask underage victims for sample photos.

What attracted attention during the participant-observation was the fact that some users directly asked others to swap images using the popular smartphone messenger WhatsApp.

The indirect offender type

While the blackmailer type acts in a direct and open way, the second main offender type tends to be covert and conspiratorial. This type, also described as "indirect" and "buddy" type, initially registers in the virtual world using false data. Because some of the virtual worlds do not compare registering IP (internet protocol) addresses, they are able to set up and operate several user accounts at the same time. One offender can thus be represented in different guises (boy/girl/age/background) in one virtual world. This is also called "multiboxing". Sometimes offenders can follow the public chat to find ways of initiating a conversation with a potential victim of their choice. The victim can then use his different avatars depending on how he wishes to appear to his victim. Usually, the offender tries to find out the age of the victim to adjust his own age accordingly. Usually the made-up age will be the same or just slightly older. During the initiating phase the offender then tries to find an emotional point of entry to the victim. This is particularly promising during puberty, if the offender shows empathy for and interest in the victim. During this phase the offender will inconspicuously try to find out about what the victim looks like and about any first sexual experiences. Should a transfer to another medium take place to continue communication there, the offender will make sure during the initiation phase that his real age or his real gender (if he changed his gender) is not revealed. On Skype, for example, he would pretend that

[5] A female avatar and nickname was used as a cover, indicating a girl aged 13.

his video camera is not working. As soon as the offender assumes that he has gained the trust of the victim, he will initiate the so-called secrecy phase. During this phase he will reveal a secret that only the two of them share, such as his true age or gender. If this does not lead the victim break off contact, the connection with the victim becomes stronger and a transition to a physical meeting, for example, is now possible.

Although police crime statistics (PCS) in Germany found a rise in reports of such crimes from 934 in 2011 by almost 50 percent to 1,406 in 2012 (BMI, 2013).

Specific example of such activities are known internationally from a great number of virtual worlds. In 2010 a 28-year-old man approached an eleven-year-old girl under the pretence of being a 12-year-old in the Dutch Habbo Hotel. He started to interact with her, connected with her through a friendship request and they fitted out a hotel room together. The two then spent a lot of time in their hotel room and led a kind of virtual family life. The offender took advantage of the fact that he was much more financially able to purchase virtual furniture. After some time, the offender initiated the so-called secrecy phase. During this phase he revealed his true age and arranged to meet the child in a hotel room. Here they engaged in sexual activities. The offender was convicted because the mother found text messages with a sexual content on the child's mobile phone (Middelburg, 2010).

Another example from the USA became the subject of intense discussion in 2011. In the MMORPG Runescape, a 54-year-old man played with a thirteen-year-old girl. It went as far as the two of them celebrating a virtual wedding in the game. Later victim and offender met in real life and engaged in sexual acts. The offender was convicted because he gave the victim a mobile phone to be able to communicate better. The mother (who had banned her daughter from owning a mobile phone) found the mobile and the saved messages containing sexual references (Parrish, 2011).

It has come to note that women are now also amongst the offenders. As early as 2009 a 42-year-old school teacher from England was arrested after grooming a 14-year-old boy in World of Warcraft (DailyMail, 2009). In another case in 2011 a 36-year-old American woman was arrested after sexually abusing a 13-year-old boy. The offender initiated the sexual abuse through the chat feature (Xbox-Live) of the game console Xbox (Kornhaber, 2011).

Overall, it is safe to say that both offender types take advantage of the special features of the virtual worlds, such as the option of offering virtual goods as payment, approaching other players through playful interaction, the games' graphics and the relatively unmonitored way of communicating.

6. The scope of the phenomenon

No specific scientific review based on recognised empirical methods of the scope of the sexual discrimination of minors in the virtual world, children's chat rooms and game environments has yet taken place. No reliable conclusions can yet be drawn about the scope of such activities. This is especially true since cases of cyber grooming (similar to other crimes of abuse) are mostly so-called control-related offences, i.e. a crime that is rarely reported by the victim and is mostly brought to light following pro-active investigations by the police. If law enforcement agencies do not attempt to find and convict online offenders themselves, the number of reports and therefore convictions will remain low. Although police crime statistics (PCS) in Germany found a rise in reports of such crimes from 934 in 2011 by almost 50 percent to 1,406 in 2012 (BMI, 2013)[6],

[6] In the German PCS the relevant entry for crimes in accordance with §176 section 4 no 3 and 4 StGB can be found under the crime code 131.400. Note that codes 131.200 and 131.300 can contain cyber grooming crimes such as sexual acts in front of a camera (BMI, 2013). Since these codes do not differentiate between classic cyber grooming offences, such as those committed in front of a camera, and offences where offender and victim are in the same room, they are

given that every day millions of children are active in online games, social networks and children's chat rooms, this number seems relatively low. An approximate estimate of the actual scope, given the above, can only be drawn from circumstantial evidence. In addition to the court decisions and reports mentioned in this article, we will in particular discuss a freely accessible survey of Fregger users, Operation Game Over of the Attorney General of the State of New York and the television programme about Habbo Hotel.

Freggers is a 3D-based social community where users (similar to Habbo Hotel) get their own virtual rooms, can furnish them and interact and communicate through their avatars in public areas and rooms. Freggers also uses very colourful and quite child-friendly designs. Each year, the website freggers-wiki.de carries out a survey with different focal points among its German-language Freggers (Freggers.de) and the English-language equivalent (Freggers.com). The latest survey was published in 2012 and particularly focuses on the experiences of users in the chat area of Freggers (Freggers-Wiki, 2011).

613 users took part in the above-mentioned survey, of which 38 percent were children under the age of (236). A further 32 percent were minors between the ages of 14 and 18 (200). The remaining users were older or did not indicate their age. What stands out is that 49 percent claimed to be female (303) and only 39 percent said they were male (242). Just under 10 percent did not indicate their gender. The survey then concentrated mostly on users' chat experiences. The survey differentiate between whether the experiences were made with an avatar looking like a female, male, adult or child. In this context 31 percent (191) of German-speaking users stated that they have been sexually harassed in Freggers (ibid.). Only 20 percent (125) of users playing with male avatars said that they were sexually harassed. This result is an indication that the choice of avatar gender could have an effect on the frequency of victimisation suffered and that users with female avatars and presumably nicknames are approached more frequently than mail avatars. At any rate, it can be noted that almost 70 percent of users of Freggers are underage and as much as one in three users report to have been sexually harassed.

Another indication for the scope of the phenomenon is supplied by Operation Game Over, an initiative of the Attorney General of the State of New York. As part of this operation, the contact details of previously convicted and registered sex offenders only in the State of New York were compared with the registration details in online games and game environments (NewYorkStateOffice, 2012-1). The reason for this operation were several sex crimes that became known in the USA where games were used as a starting point (Fahey, 2011). The prosecuting authorities gained access to the data records because of a New York law requiring previously convicted sex offenders to reveal personal data including provider information and email addresses. The prosecuting authorities passed on these email addresses to cooperating game companies such as Microsoft, EA-Games, Blizzard, Disney, Sony and Apple. The result of the first stage of the operation in April 2012 was that 3,580 accounts were registered by sex offenders in the games of the cooperating companies and were subsequently banned. In a second stage at the end of December 2012, another 2,100 accounts were banned (NewYorkStateOffice, 2012-2). This means that in total 5,680 accounts by sex offenders were found in the participating games.

The result of the first stage of the operation in April 2012 was that 3,580 accounts were registered by sex offenders in the games of the cooperating companies and were subsequently banned.

A number of aspects need to be taken into account when assessing the operation. For example, it cannot be simply assumed that each one of the offenders registered in order to seek sexual interaction with minors.

not taken into consideration.

Even among previously convicted sex offenders, the majority is likely to have registered out of interest in the game. Conversely, only the figures for registered sex offenders from one state were taken into consideration and only for a limited number of games. For example the „game companies“ BigPoint, Zynga, Sulake, Gameforge, Riot Games, Turbine and Linden Labs were not represented.

Another aspect should also be taken into consideration. At the beginning of June 2012, British channel Channel 4 reported about the huge number of sexual assaults by paedophiles in Habbo Hotel (Channel4, 2012). As a result of public pressure, Sulake, the operator of Habbo Hotel, was forced to disable all chat in Habbo (Habbokritik, 2012). The fact alone that Sulake initially saw no other way of handling the sexual assaults than to no longer allow any communication is evidence of the sheer scale of sexual harassment in Habbo Hotel.

The main problem both systems have is that they have not yet managed a paradigm shift towards reflecting the risks of communication and interaction of online games.

7. Protection of children and minors

From the point of view of the protection of children and minors, almost all virtual worlds have the same faults. If youth protection mechanisms are in place, they are usually based on users specifying their age when registering or report functions that are part of the game. For example, a warning will be displayed to children when they want to start communicating with an adult. The age that is used when making the comparisons is the one that has been entered voluntarily and unmonitored at the time of registration. It's quite obvious that this system can easily be dodged simply by giving the wrong age. Another obvious point of criticism is that typically the reaction mechanisms of the operators boil down to reacting rather than acting. For example, you often find requests that children and other users should use the reporting function or alarm button as soon as they encounter sexual harassment. This means, however, that in the worst case the child will have already read some more or less explicit sexual content and has therefore already been victimised. What's more, the contact persons of virtual worlds (game masters or adminstrators) are recruited from among the users of the world, presumably for reasons of cost. And it looks as if the staff serving as first point of contact in a case of sexual victimisation has not been particularly carefully selected for this task, been made aware of the relevant issues or even trained. This is partly due to the fact that no officially binding regulations are in place. It is all the more perplexing that the German state considers it necessary to penalise cyber grooming according to §176 IV StGB especially in the case of children (up to 14 years), but at the same time the German youth protection system does not have an age rating ‚from 14 years‘.

The issue of age ratings therefore needs further scrutinising. This in particular applies to the criteria of the entertainment software self-regulation body (USK) in the German-speaking region and the Pan European Gaming Information System (PEGI) internationally. The main problem both systems have is that they have not yet managed a paradigm shift towards reflecting the risks of communication and interaction of online games. The organisation USK in particular, which is responsible Germany and some of the Austrian provinces, is by law only responsible for games that are provided on data carriers and even then only for the question whether these games contain factors that compromise or arrest development (mostly violent or pornographic content[7]). For purely online-based virtual games (such as browser and social games, game applications, most life simulations and MMOPRGS as well as online worlds for children) the USK is not responsible at all, so that no official age ratings are applied here. Online games that do get an age

[7] For a detailed presentation of the German youth protection systems and their weaknesses see the article “Kinder- und Jugendschutz vor den Herausforderungen des Web 2.0”.

rating from the USK, are, simply put, examined as to their pornographic and violent content, which in online games (that often focus on a childish look) is precisely not the case. What's also problematic is that in this situation the operators themselves assess the age rating for the games, in order to obtain a so-called electronic labelling that's not visible to normal users for an automatic alignment match with youth protection programmes. As a result these online games are often approved for children. Another issue are online modes of computer games, which specifically provide for communication between users. These cannot be taken into consideration by the USK age ratings because there is a lack of legal foundation. In practice, the result is that computer games that are suitable for children such as Little Big Planet (here in the PSP Vita version) are approved from 0 years and only on the back of the package is there a little note referring to the "network mode 2 – 4", the online mode that allows you to play with others. Parents who buy such a game in good faith, relying on the USK guidelines, are presumable less aware of its inherent communication risks.

PEGI takes a different direction here by at least providing its own information graphic for online games based on data carriers. PEGI also offers a kind of voluntary safety certificate, the "PEGI Online Safety Code (POSC)" for online games companies that meet a particular set of safety guidelines (PEGI, 2012). This procedure, however, also has faults in its current form. Given that the safety certificate is on a voluntary basis, a great number of companies (including Riot Games, Zynga, BIGPoint) are not taking part. The POSC also contains no effective mechanisms to prevent the risks inherent in interaction and communication. Rather, attention is paid to there not being any content that is harmful to youth together with the introduction of the relevant reporting features. These mechanisms, however, only serve to report victimisations already suffered, not to prevent them.

Rather, attention is paid to there not being any content that is harmful to youth together with the introduction of the relevant reporting features. These mechanisms, however, only serve to report victimisations already suffered, not to prevent them.

Using the reaction of Sulake to the above-mentioned TV report aired on British Channel 4 as an example, which disclosed the serious faults there, the powerlessness when it comes to implementing an effective youth protection legislation is to be emphasised. To obtain a better understanding of the issue it is also useful to know that Habbo Hotel is a kind of franchise, which operates various independent language versions under the umbrella of Sulake. It appears that youth protection has increasingly been neglected over the years (Habbokritik, 2012). For example, foreign moderators were used who don't speak the site's language (ibid.). In reaction to these events, Sulake promised to improve its youth protection measures massively. One of these measures was to be a safety quiz for the German-language Habbo (five simple questions that have to be answered), a certain period during which chat is not enabled[8] (half an hour; this regulation is not in place in the English-language versions of Habbo for example), an improved blacklist of words that are not allowed to be used and integrating the community more into the control process by appointing guards. The only noticeable effects were that the blackmailer types (as already described) started their sexual interactions in a covert way, or that they were banned more quickly following a communication attempt and have to reregister. When they used to write something like *"which girl with cam wants sex"*, following the new safety measures they might now write *"which girls wants to see a MOHA (morning hard-on)"*. Another phenomenon that was observed more frequently was that the term Skype was no longer written in one window, but rather the individual letters were put in separate

[8] Habbo Hotel once again abolished this safety mechanism of an enforced waiting time after registering before being able to contact other users in February / March, so that creating a new avatar after a ban can be done without a problem. This has led to a noticeable increase in sexual communication in the German-language Habbo.

Until now, online games and virtual game environments for children have not been on the security policy agenda, despite their huge popularity among minors and the possibilities of anonymous communication among users that they provide.

windows; overall it was quite clear what that was supposed to mean. On the other hand, it can be noted that offenders were obviously reported and banned earlier in cases of sexual communication than before and that offenders had to change avatars more often in the context of sexual communication with minors, because their avatar was removed from the game. This was more of an annoying nuisance for the offenders rather than a true obstacle. The offender was able to and still can now easily avoid them by either logging in with a new avatar or by being represented with several avatars to begin with through multiboxing. The true weak points, namely that there is no sensible age and ID verification process in Habbo Hotel, were not addressed by Sulake. The Habbo Hotel community also sees it this way and describes the measures taken so far as ineffective (ibid.).

8. Summary

Security agencies and politicians around the world now accept that social networks such as Facebook and Google Plus are platforms that are of criminological relevance and are developing policing measures in the form of response and prevention programmes (Denef et. al., 2012). Until now, online games and virtual game environments for children have not been on the security policy agenda, despite their huge popularity among minors and the possibilities of anonymous communication among users that they provide. This is also well reflected in the fact that Sulake, the operator of Habbo Hotel, was admitted by the European Commission at the end of 2011 as a member in the digital coalition of leading technology and media companies for the creation of an internet that is safe and friendly for children (Europe, 2011). A simple inspection of Habbo Hotel or an internet search would have revealed at that time the huge number of cases of sexual harassment that users are and were exposed to. However, virtual worlds and online games in particular are still not sufficiently accepted as criminal platforms and therefore ultimately victimisation (except for a brief flurry of interest in Second Life in the years 2007 / 2008) (Krebs & Rüdiger, 2010).

So far the operators are not legally obligated to a sufficient extent to effectively ensure the protection of minors, for example by forcing users of children's games or games that are approved for children to give up their anonymity (such as by using a postal ID process). It appears necessary here to launch a legislative initiative that should be compulsory specifically for Germany as well as for the European market, both in order to prevent competitive distortion and to provide media protection for children and young people that is as effective as possible.

The lack of political and social attention received by this subject matter is all the more problematic as other entities of social control (including parents and legal guardians) do not always understand or are able to properly contextualise the risks associated with virtual worlds because of a lack of knowledge about the media in question. In practice, this means they are not sufficiently aware of the problem, which in turn can lead to an increased rate of victimisation among minors. The government must not ignore this and should instead act. How this can be done is exemplified by the Dutch police in Habbo Hotel with their project DigiKids (see article "Dutch police, vision on youth and internet"). This has to become common practice, as this is currently the case with the classic social networks.

Given the rapid increase of the social, economic and societal significance of virtual worlds, a political discussion especially about their inherent social interaction and communication risks seems unavoidable. Pilot initiatives, such as the holding of an event on child and youth protection by the Minister of the Interior of the State of Brandenburg in September 2012, show that a shift in thinking is underway (Woidke, 2012).

Sources and bibliography

Blizzard (2010): World of Warcraft subscriber base reaches 12 million worldwide. Available online at http://eu.blizzard.com/en-gb/company/press/pressreleases.html?id=2443926 last checked on 7 February 2013.

Breichler, Inge / Knierim, Katja / Lübbesmeyer, Nina (2009): Chatten ohne Risiko? Sicher kommunizieren in Chat, Messenger und Community. Jugendschutz.net, Mainz.

Bullens, Ruud (1995): Der Grooming-Prozess – oder das Planen des Missbrauchs. In: Marquardt-Mau, B. (ed.): Schulische Prävention gegen sexuelle Kindesmisshandlung. Grundlagen, Rahmenbedingungen, Bausteine, Modelle, Munich.

Federal Ministry of the Interior (BMI) (2013): police crime statistics 2012, Berlin

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom-1) (2012): Zahlungsbereitschaft für Online-Games steigt. Available online at http://www.bitkom.org/files/documents/bitkom-presseinfo_online-gaming_07_11_2012.pdf, last checked on 7 February 2013.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom-2) (2012): Gaming wird immer populärer. Available online at http://www.bitkom.org/de/presse/74532_73098.aspx, last checked on 8 February 2013.

Bundesverband Interaktive Unterhaltungssoftware e. V. (BIU) (2011): Marktzahlen - Virtuelle Zusatzinhalte. Available online at http://www.biu-online.de/de/fakten/marktzahlen/virtuelle-zusatzinhalte.html, last checked on 8 February 2013.

Federal Association of Interactive Entertainment Software (BIU) (2012): Games-Report 2012. Facts and figures about the German games industry. Available online at http://www.biu-online.de/fileadmin/user_upload/pdf/games_report_2012_druck.pdf, last checked on 8 February 2013.

Chalk, Andy (2010): Gamer Arrested For Using WoW Gold to „Groom“ Underage Boys. Available online at http://www.escapistmagazine.com/news/view/98088-Gamer-Arrested-For-Using-WoW-Gold-to-Groom-Underage-Boys, last checked on 8 February 2013.

Channel 4 (2012): Should you let your child play in Habbo Hotel? Channel 4. Available online at http://www.channel4.com/news/should-you-let-your-child-play-in-habbo-hotel, last checked on 8 February 2013.

Choo, K.(2009). Australian Institute of Criminology Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences. Available online at http://www.aic.gov.au/documents/3/C/1/%7B3C162CF7-94B1-4203-8C57-79F827168DD8%7Drpp103.pdf, last checked on 7 February 2013.

Cole, Helena / Griffiths, Mark D. (2007): Social Interactions in Massively Multiplayer Online Role- Playing Gamers. In CyberPsychology & Behavior Volume 10, Number 4, p. 575 – 583.

Daily Mail (2009): Primary school teacher facing jail for sending lewd texts to schoolboy after grooming him on World of Warcraft. Available online at http://www.dailymail.co.uk/news/article-1115603/Primary-school-teacher-facing-jail-sending-lewd-texts-schoolboy-grooming-World-Warcraft.html, last checked on 8 February 2013.

Denef, Sebastian; Kaptein, Nico; Bayerl, Petra S.; Ramirez, Leonardo (2012): Best Practice in Police Social Media Adaptation. Composite Comparative Police Studies in the EU.

Durkheim, E.(1965). Kriminalität als normales Phänomen. In: Ibid., Die Regeln der soziologischen Methode. 2nd edition Neuwied 1965. Reprinted in: Sack, F./König, R. (eds.): Kriminalsoziologie. 2nd edition Frankfurt 1974, p. 3-8.

Dwell (2012): Second Life Statistical Charts. Available online at http://dwellonit.taterunino.net/sl-statistical-charts, last checked on 8 February 2013.

Erenli, K.(2008). Virtuelle Welten – Ausgewählte Aspekte des Vertrags- und Urheberrechts unter Berücksichtigung praxisrelevanter Problemstellungen. University of Vienna, University course in information rights and legal information.

Europa (2011): Self regulation: responsible stakeholders for a safer Internet. Available online at http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm, last checked on 8 February 2013.

Fahey, Mike (2011): Self-Professed Furry Charged With Xbox Live Child Abuse. Kotaku. Available online at http://www.kotaku.com.au/2011/04/self-professed-furry-charged-with-xbox-live-child-abuse/, last checked on 8 February 2013.

Finkelhor, David / Mitchell, Kimberly J. / Wolak, Janis / Ybarra, J. Mitchell (2008): Online "Predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment. In American Psychologist Vol. 63, p.111 – 128.

Freggers-Wiki (2011): Freggers Umfrage 2011. Available online at http://www.freggers-wiki.de/umfragel/2011_freggers/, last checked on 8 February 2013.

Fritz, Jürgen; Lampert, Christian; Schmidt, Jan-Hinrik; Witting, Tanja (2011): Kompetenzen und exzessive Nutzung bei Computerspielern: Gefordert, gefördert, gefährdet. Zusammenfassung der Studie. Hans Bredow Institute. Hamburg (publication series media research of the State Institute for Media NRW (LfM)). Available online at http://www.hans-bredow-institut.de/webfm_send/563, last checked on 8 February 2013.

HabboKritik (2012): Große Stummschaltung ohne Effekt. Da Sulake die Stummschaltung langsam wieder aufhebt, ziehen wir ein Fazit. Available online at http://habbokritik.de/artikel/2447, last checked on 8 February 2013.

InStat. (2011). Virtual Goods in Social Networking and Online Gaming. Ed. v. INSTAT. Available online at http://www.instat.com/abstract.asp?id=212&SKU=IN1004659CM, last checked on 8 February 2013.

Katzer, Catarina (2007): Gefahr aus dem Netz. Der Internet Chatroom als neuer Tatort für Bullying und sexuelle Viktimisierung von Kindern und Jugendlichen. PhD thesis, University of Cologne.

KidsverbraucherAnalyse (KidsVA) 2012 (2012): Die Markt-Media-Studie für junge Zielgruppen im Auftrag des Egmont Ehapa Verlages GmbH. Berlin.

Kinder+Medien, Computer+Internet Studie (KIM) 2010 (2010): Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger in Deutschland. MediaEducation Research Association Southwest. Available online at http://www.mpfs.de/fileadmin/KIM-pdf10/KIM2010.pdf, last checked on 28 February 2013.

Kornhaber, Spencer (2011): Lake Forest Woman Arrested on Suspicion of Sex with 13-Year-Old Boy. LakeforestPatch. Available online at http://lakeforest-ca.patch.com/articles/lake-forest-woman-arrested-on-suspicion-of-sex-with-13-year-old-boy, last checked on 8 February 2013.

Krebs, C., Rüdiger, T.G.(2010). Gamecrime und Metacrime. Strafrechtlich relevante Handlungen im Zusammenhang mit virtuellen Welten. Frankfurt, M: Verl. für Polizeiwiss.

Leschni (2012): PlayStation 3: Sony verkündet 70 Millionen verkaufte Konsolen. Play3.de. Available online at http://www.play3.de/2012/11/16/playstation-3-sony-verkundet-70-millionen-verkaufte-konsolen/, last checked on 8 February 2013.

Livingstone, Sonka; Haddon, Leslie Görzig Anke; Olafsson, Kjartan (2011 - 1): Risks and safety on the internet. The perspective of European Children. Key findings from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. Available online at http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Executive_Summary_Full_Findings.pdf, last checked on 9 February 2013.

Livingstone, Sonja; Haddon, Leslie; Görzig, Anke (2011 - 2): EU Kids Online aims to enhance knowledge of the experiences and practices of European children and parents regarding risky and safer use of the internet and new online technologies, in order to inform the promotion of a safer online environment for children. Available online at http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/EUKidsOnlineIIReports/Final%20report.pdf, last checked on 9 February 2013.

District court Saarbrücken (LG Saarbrücken) (2011). Reference no.: 10 S 60/10 dated 22 June 2011.

Meyfarth, M. (2007). Zusammenspiel virtueller und realer Raum Beispiele und Möglichkeiten. Institute of Electronic Business. Available online at http://www.mr-meyf.de/docs/Zusammenspiel%20virtueller%20und%20realer%20Raum.pdf, last checked on 10 February 2013.

Middelburg (2010). Judgement in the courts of the Netherlands. Reference no: 2010/12/700056-10 dated 3 November 2010.

New York State Office (2012-1): Attorney General: „Operation: Game Over“. Purges Thousands Of Sex Offenders From Online Video Game Networks. Press release dated 5 April 2012. New York. Available online at http://www.ag.ny.gov/press-release/ag-schneidermans-operation-game-over-purgesthousands-sex-offenders-online-video-game, last checked on 8 February 2013.

New York State Office (2012-1): Attorney General Schneiderman's "Operation Game Over" Continues With Thousands Of Additional Sex Offenders Purged From Online Gaming Platforms", press release dated 19 December 2013. New York. Available online at http://www.ag.ny.gov/press-release/ag-schneiderman%E2%80%99s-%E2%80%9Coperation-game-over%E2%80%9D-continues-thousands-additional-sex-offenders, last checked on 8 February 2013

Pakalski, Ingo (2012): Fast jedes dritte Handy in Deutschland ist ein Smartphone. Available online at http://www.golem.de/news/mobilfunk-fast-jedes-dritte-handy-in-deutschland-ist-ein-smartphone-1205-91858.html, last checked on 8 February 2013.

Parrish, Kevin (2011): Man, 54, ‚'Marries" Teen in RuneScape, Arrested. Available online at http://www.tomsguide.com/us/RuneScape-John-W-Phillips-MMORPG-Sexual-Assault, news-10069.html, last checked on 8 February 2013.

PcGames (2012): World of Warcraft: 30 Prozent Anteil am Umsatz von Activision-Blizzard - Ist der Publisher zu abhängig von WoW? Published by PcGames. Available online at http://www.pcgames.de/World-of-Warcraft-PC-16678/News/World-of-Warcraft-30-Prozent-Anteil-am-Umsatz-von-Activision-Blizzard-1015757/, last checked on 8 February 2013.

PEGI (2012): Was ist der POSC. PEGI Online. Available online at http://www.pegionline.eu/de/index/id/37, last checked on 8 February 2013.

Pfeiffer, Christian; Mößle, Thomas; Kleimann, Matthias; Reh-bein, Florian (2009): Computerspielabhängigkeit und „World of WarcraftWorld of Warcraft“. Fünf Thesen zu politischen Folgerungen aus aktuellen Forschungsbefunden des KFN. Edited by the Lower Saxony Criminological Research Institute. Available online at http://www.kfn.de/home/WoW_Thesen_zu_politischen_Folgerungen.htm, last checked on 8 February 2013.

Phagura, Sabi (2012): Police worker who coaxed children into performing webcam ‚sex shows‘ is jailed Read more: http://www.dailymail.co.uk/news/article-2199095/Police-worker-coaxed-children-performing-webcam-sex-shows-jailed.html#ixzz2KWqVPipz. Available online at http://www.dailymail.co.uk/news/article-2199095/Police-worker-coaxed-children-performing-webcam-sex-shows-jailed.html#axzz2KWqSbzgL, last checked on 28 February 2013.

Pingdom (2012): Internet 2011 in numbers. Available online at http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/, last checked on 18 February 2013.

Rumpf, H. J., Meyer, C. & John, U. (2011): Prävalenz der Internetabhängigkeit (PINTA) Bericht an das Bundesministerium für Gesundheit. Available online at http://drogenbeauftragte.de/fileadmin/dateien-dba/DrogenundSucht/Computerspiele_Internetsucht/Downloads/PINTA-Bericht-Endfassung_280611.pdf , last checked on 8 February 2013.

Rüdiger, T.-G.(2012). Cybergrooming in virtuellen Welten. Neue Chancen für Sexualtäter. In: Deutsche Polizei Ausgabe 02/2012, p. 31–37.

Rüdiger, T.-G. (2013-1) Gamecrime und Metacrime - Kriminogene Aspekte virtueller Welten, in: Bigl/Stoppe (eds) ‚Playing with Virtuality', Frankfurt: Peter Lang, p. 397 – 417.

Rüdiger, T.-G. (2013-2) "Legendierte teilnehmende Beobachtung im deutschsprachigen Habbo Hotel am 28.02.2013 im Zeitraum von 13:00 – 16:00 Uhr und am 02.03.2013 im Zeitraum von 12:00 – 12:40 Uhr", (undercover participant-participation in the German-lkanguage Habbo Hotel on 28 February 2013 between 1 and 4 p.m. and on 2 February 2013 between noon and 12.40 p.m.) tabular assessment using screenshots and video documentation (unpublished).

Shaw, Gillian (2012): Amanda Todd: Her story and legacy live on Worldwide, anti-bullying campaigns have been launched following teenager's suicide. Available online at http://www.vancouversun.com/news/Amanda+Todd+story+legacy+live/7756533/story.html.

Sulake (2012). Check in to check it out! Available online at http://www.sulake.com/Habbo/index.html?navi=2.1, last checked on 8 February 2013.

Tagesspiegel (2012): Zynga-Desaster könnte Facebook-Zahlen belasten. Der Tagesspiegel. Available online at http://www.tagesspiegel.de/wirtschaft/soziale-netzwerke-zynga-desaster-koennte-facebook-zahlen-belasten/6924488.html, last checked on 8 February 2013.

Ybarra, Michel / Mitchel, Kimberly (2005): Exposure to Internet Pornography among Children and Adolescents: In CyberPsychology & Behavior Volume 8, Number 5, p. 473 – 486.

YouGov (2012): Fast jedes zweite Kind unter 10 Jahren besitzt ein eigenes Mobiltelefon. Available online at http://cdn.yougov.com/r/19/2012_07_PM%20Kinder%20Handy.pdf, last checked on 8 February 2013.

Woidke, Dietmar (2012): Woidke fordert mehr Schutz für Kinder und Jugendliche vor sexuellen Übergriffen bei Online-Spielen, Pressemitteilung des Ministerium des Innern des Landes Brandenburg vom 19.09.2012. Available online at http://www.internetwache.brandenburg.de/sixcms/detail.php?gsid=land_bb_polizei_internet_01.c.11215104.de, last checked on 8 February 2013.

About the author

Thomas-Gabriel Rüdiger (32), married and father of two daughters, earned his Master of Arts degree in criminology from the University of Hamburg. He is a criminologist at the Institute for Police Science at the University of Applied Science of the Brandenburg Police, where his main research focus is in the area of risks of interaction in the social media and how the police should deal with them. He is currently working on a PhD at the University of Potsdam, where he participates in an interdisciplinary project on the sexual victimisation of minors in virtual worlds.

Cybergrooming in the context of criminal prosecution

State Prosecutor Thomas Schulz-Spirohn and District Court Judge Kristina Lobrecht

Abstract

Cybergrooming, a criminal offence in Germany since 2004, is increasingly coming into the focus of the media and the public debate. Alongside the legal issues of whether online games and chats on the Internet actually satisfy the linguistically obsolete mens rea pursuant to section 176 (4) (3) German Criminal Code *(Strafgesetzbuch,* StGB), both the behaviour of the victims in reporting offences and the technical and staffing capabilities of the law enforcement agencies pose difficulties in effectively prosecuting this offence. Alongside the comparison of the German offence with the equivalent Austrian criminal law, the article explains the measures through which the actual purpose of the European Directive 2011/92/EU on "combating the sexual abuse and sexual exploitation of children and child pornography" of 13 December 2011 can be achieved.

1) Introduction

Cybergooming, i.e. the targeted approach of children and young people on the Internet with the aim of initiating sexual contact, has been punishable in German criminal law since the Act Amending Sexual Offences (*Sexualdelikte-Änderungs-Gesetz*) dated 27 December 2003 came into force on 1 April 2004, at least insofar as such acts are aimed at "children" as defined under the German Criminal Code. German legislation considers "children" to be persons under the age of 14 (section 176 StGB), i.e. persons who at the time of the act had not reached the age of 14. This "age of consent" varies considerably within the European Union. For instance, the age of consent is 12 in Malta[2], 17 in Ireland[3] and 18 in the EU candidate country Serbia[4]. Around the world the age of consent ranges from the start of puberty (around 10 years of age in Yemen) to 18 (in certain US states[5]). Close scrutiny is therefore needed to determine the exact age of the victim as the precise date of birth of migrants may be questionable and German law affords no protection from cybergrooming to people over 14 years of age, plus the penal provisions aimed at the protection of young people, which will also be considered, are subject to additional conditions.

Around the world the age of consent ranges from the start of puberty (around 10 years of age in Yemen) to 18 (in certain US states).

2) Offence

Since the introduction of the offence the legal basis for combatting this criminal phenomenon in German criminal law has been section 176 (4) (3) StGB.

It reads:

"Section 176 Child abuse

[1] The criminological aspects of the manifestations of cybergrooming have already been specifically described in the article by Mr. Thomas-Gabriel Rüdiger, so this article will deal solely with the legal dimension with a focus on German criminal law.

[2] http://www.welt.de/politik/deutschland/article7319676/Vatikan-erlaubt-Sex-mit-Kindern-ab-zwoelf-Jahren.html on the topic of the "age of consent"

[3] Report of the European Commission dated 16 November 2007

[4] Travel and safety advice of the German Foreign Office (Auswärtiges Amt) for Serbia

[5] Travel and safety advice of the German Foreign Office for the USA

> *[...]*
> *(4) Whosoever*
> *3. presents a child with written materials (section 11(3)) to induce him to engage in sexual activity with or in the presence of the offender or a third person or allow the offender or a third person to engage in sexual activity with him,[…] shall be liable to imprisonment from three months to five years.*
> *(6) The attempt shall be punishable; this shall not apply to offences under subsection (4) Nos 3 and 4 [...] above."*

The murderer who buys an axe does not, or cannot, expect, that the victim will agree to the act and will suddenly be standing there before him.

This offence, complete with a number of vague legal concepts and worded in a less than contemporary manner, is intended – if we look at the justification for the law – to cover the offence of cybergrooming.

The legislative materials[6] refer to a press report in the Süddeutsche Zeitung of 1999 that describes the approach of (American) Internet users who use chat rooms to arrange meetings with children with the aim of sexually abusing them. Section 176 (4) (3) StGB is intended to criminalise contact driven by such motivations. Under the criminal provisions in force to date, there has been no way of prosecuting such preparatory acts taking place prior to the direct initiation of sexual abuse.

a) Criticism of the offence

Legal academic literature continues to raise huge objections to the introduction of this offence. Although public debate acknowledges the need to protect children from the dangers of new media – in particular the Internet – positive opinions in the legal literature on the offence for prosecuting cybergrooming are few and far between. Accusations of absurdities, inconsistencies and nonsensical results are levelled[7].

The conclusion[8] is that the offence is a *"well-meant, toothless attempt to deal with an uncontrollable form of communication"* and that its *"character is little more than a symbolic threat"*, *"Cybergrooming is not even punishable in Germany. Protect our children at last"*[9] through ... *is not always punishable in Germany, i.e. when it is just chatting"*[10] right up to *"even socially acceptable conduct is penalised"*.[11] A particularly common argument is based on the contention that criminalising acts long before an actual breach of the legally protected right – the right to sexual self-determination and the protection of children – is a step too far.[12] It is also astonishing, so the argument continues, that the preparatory acts for a murder under section 211 StGB are not criminalised, as long as they do not lead to the direct commission of the offence.[13] However, these arguments are unconvincing. The intention of the legislator to make children the subject of special protection can be seen in a range of laws in which for example homicides are ranked lower, such as the periods before a conviction is deemed spent in the Act on the Central Registry and Educational Register (*Gesetz über das Zentralregister und das Erziehungsregister*, BZRG).[14] The acts covered by section 176 (4) (3) StGB are also not comparable with the non-punishable preparatory acts as defined in section 211 StGB. The murderer who buys an axe does not, or cannot, expect, that the victim will agree to the act and will suddenly be standing there before him. This is

[6] Bundestag document 15/350, p. 177

[7] Summarising Hube, Kriminalistik 2/ 2011, p. 73

[8] Fischer, StGB, 59th ed., section 176, margin note 15

[9] Tatort Internet, RTL II

[10] Hörnle, Leipziger Kommentar zum Strafgesetzbuch, 12th ed., section 176 StGB, margin note 87 with further notes

[11] Paraphrasing Perron/Eisele in Schönke/ Schröder, StGB, 28th ed., section 176, margin note 14

[12] Hörnle, op.cit.

[13] Cf. StrafO 2004, 265, 267

[14] Cf. section 46 (3) BZRG in relation to section 46 (4) BZRG

different in the case of cybergrooming. In many cases the anonymity of the Internet enables the offender to mask his true intentions and encounter an innocent counterpart who does not recognise the risks or the consequences of his/her acts.[15] This real risk to children can only be tackled by means of protection under the criminal law that kicks in at a sufficiently early stage and suitable preventative measures.

In many cases the anonymity of the Internet enables the offender to mask his true intentions and encounter an innocent counterpart who does not recognise the risks or the consequences of his/her acts.

b) Inducing

According to section 176 (4) (3) StGB the prerequisite for the commission of the offence is "inducing" children through the presentation of "written materials". The very determination of when an offender has induced a child in the manner defined by this Act presents certain difficulties in the absence of case-law from the highest judicial instance in relation to section 176 (4) (3) StGB. Considering the case law of the German Federal Supreme Court (*Bundesgerichtshof*) – in fact in respect of a different offence, namely the old offence of human trafficking under section 180 b I sentence 2 StGB (now section 232 StGB) – which contained the element of "inducing", this is understood to be the exertion of a direct psychological influence that is characterised by a degree of tenacity, such as repeated urging, persuasion, promising, arousing curiosity, use of authority, deception, intimidation and threats.[16] This apt definition, which contains a restricting and clearly delimited depiction of punishable conduct to satisfy the principle of legal certainty, can also be used as a definition pursuant to section 176 (4) (3) StGB according to prevailing opinion.[17]

However, this also shows that a one-off inducement of children, which is not continued for whatever reasons, does not represent punishable inducement as defined by this Act. Because the attempt is not a punishable offence, one-off inducement cannot be punished.

c) Concept of written materials

The inducement of a child must be by way of "written materials". Influencing a child by means of a direct personal communication or a telephone call is not covered by the section. As for the concept of written materials section 176 (4) (3) StGB in turn refers to section 11 StGB, which for its part contains what is called an equalisation clause in section 11 (3) StGB.

Section 11 (III) StGB reads:
"[...] Audiovisual media, data storage media, illustrations and other depictions shall be equivalent to written material in the provisions which refer to this subsection."
It is generally acknowledged that chat protocols or communications during an online game do not represent written material as defined by section 11 StGB. The question raised in the public debate as to why something written does not amount to written material can only be explained by the strict criteria under section 11 StGB. This requires the concept of "written material" to be an embodiment and therefore only describes the written word on paper or other transportable material that can be readily perceived by anyone.[18]

It therefore follows that in the case of "cybergrooming" solely the concept of "data storage media" can be relevant for establishing the offence. The concept of "data storage media", which was not inserted into section 11 (3) StGB until 1997,[19] is initially understood to mean storage media for electronic, electro-magnetic, optical, chemical or other

[15] Cf. also the article by Rüdiger by way of summary

[16] cf. BGHSt 45, 158; BGH NStZ 2000, 86

[17] cf. NStZ 2011, 455; BGHSt 29, 30; NStZ 1991, 45

[18] cf. Prof. Dr. Marco Gercke, Aufsatz "Was wirklich strafbar ist-vielleicht" dated 20 October 2010 from "Legal Tribune-Online"

[19] inserted by Art. 4) (1) German Information and Communication Services Act (Informations- und Kommunikationsdienste-Gesetz, IuKDG) dated 22 July 1997 [BGBL. I 1870]; RegE BT-Drs. 13/7385, 35

recording of data, which embody intellectual content.[20] According to prevailing opinion, this also covers the non-permanent electronic internal memory of computers of all types and network servers.[21] Communications whose content is stored in an internal memory for a longer period also fall within the concept of written materials. Contacts via e-mail therefore satisfy the element of the offence of "inducement through written materials", as do for example contacts via text message.

However, what is problematic and controversial is the question of whether contacts in online games, life simulation games, chat rooms or social networks such as ICQ, Skype or Facebook fall within the concept of "data storage media". What these have in common is that they are transmitted in real time with just temporary storage in the internal memory.

However, here we can see that the concept of written materials used by the German lawmakers is no longer in keeping with current technical developments and therefore ought to be replaced as soon as possible.

One way of looking at this is that at least temporary storage in the internal memory counts.[22] In the case of a real-time transmission without such an intermediate inspection – as in the case of all chats or online games – there is no inducement thorough written materials as only a brief storage in the internal memory takes place.[23]

This extreme interpretation contradicts both the legislator's clear intention to create an offence to criminalise conduct on the Internet that involves inducement through the written word, i.e. through the contents of thought; and moreover the interpretation strips the offence of any practical benefit.

This is because, even in the case of real-time transmission, the text is stored at least temporarily on the offender's PC before the text is sent.[24] If the written text can be stored and printed out by way of a "screenshot", it can be embodied and read out in court proceedings pursuant to 249 et seq. German Code of Criminal Procedure (*Strafprozeßordnung*, StPO). Through the element of "embodiment" the written word on the Internet also acquires parity with regular writing as defined by section 11 StGB and therefore is in keeping with the intention of the lawmakers.

However, here we can see that the concept of written materials used by the German lawmakers is no longer in keeping with current technical developments and therefore ought to be replaced as soon as possible.

d) Commission of the offence

The offence is committed as soon as the child has taken note of the written material(s). It is irrelevant whether the offender is successful, i.e. the child meets him. "Inducement" is therefore also given if the child does not react in the way desired by the offender.

e) Intent issue

In terms of the mens rea, the offender needs to intend the result to be sexual acts involving the child with or in front of the offender or a third party a criminal act for pursuant to section 176 (4) (3) StGB to be made out. The intention for the child to engage in sexual acts on his/her own is therefore insufficient under the wording of the law, as is the intention of the offender to engage in exhibitionist acts in front of the child or to conduct sexually-related conversations via the Internet in later communications.

If the offender communicates in the hope of finding a child seeking sexual contact of his/her own accord, he is not acting with

[20] Cf.. Thomas Fischer op. cit., paragraph 11, margin note 36.

[21] Cf. BGHSt 47, 55 et seq.; JR 2000, 125; NJW 2000, 1051

[22] Hörnle, op. cit, BGH NJW 2001,3558, NJW 2010, 1893, Radtke in Münchener Kommentar zum StGB, 2nd ed. on section 11, margin note 147

[23] Radtke op. cit.

[24] Cf.. Renzikowski, Münchener Kommentar zum Strafgesetzbuch, 2nd ed., section 176, margin note 39

the intention of enticing the child to engage in sexual acts. This is the unanimous opinion in the academic discourse on criminal law.[25]

In order for an offence to be made out under section 176 (4) (3) StGB, a communication that outwardly appears harmless is sufficient if the offender intends to entice the child to engage in sexual acts, and the communication has crossed the threshold of tenacity.

This poses a real problem for forensic practice in deciding about corresponding cybergrooming cases. Unless there is a confession by the offender, evidence of this internal offence can only be adduced painstakingly using circumstantial evidence. A skilled defence strategy specifically in relation to the issue of intent can prevent a conviction in these cases. Without corresponding embodiments that can be read out in court or witnesses (parents or other children) who were present at the time of the communication, the production of evidence is thus difficult, but not impossible. According to section 176 (4) (3) StGB what is termed conditional intent (*Eventualvorsatz*) is sufficient to satisfy the mens rea requirement, i.e. the offender merely needs to consider it possible that he is communicating with a child. If he communicates with the child nonetheless, he knowingly takes this into account or is accepts the possibility and therefore satisfies the mens rea requirement.[26] This prevents convictions from failing if an accused states: *"I thought this was all made-up, a role-play, I thought it was actually an adult."* This is because this statement can be tested against the established or known facts during the trial. What needs to be assessed here are the social networks or virtual worlds on which the communication took place, the accused's sexual preferences, the social networks or games he plays on.

f) Conclusion

In summary, an initial legal review has shown that communication-based cybergrooming has been covered under the criminal law of section 176 (4) (3) StGB since 2004 and is punishable, in particular it satisfies the provisions of "Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA" dated 4 November 2011. We should also consider that the range of sentences of section 176 (4) (3) StGB is considerably wider than the Directive requires (the Directive suggests as maximum penalty of one year), and Germany introduced this offence before it was obliged to do so.

3) Comparison between the German and Austrian offence

In sum the aforementioned Directive produced various new criminal offences in the European countries, whereby their formulations are of particular interest. There follows a comparison with the Austrian provision.

Section 208a of the Austrian Criminal Code (*Strafgesetzbuch Österreich*, Austrian StGB), introduced by the amendment of the Criminal Code in 2011 and taking effect on 1 January 2012, criminalises cybergrooming and other preparatory acts.

Section 208a StGB reads:

> *"(1) Whosoever, with the intention of committing a punishable act with an under-age person pursuant to sections 201 to 207a (1) line 1*
> *1. by way of a telecommunication, using a computer system or*
> *2. otherwise, concealing his intention, suggests a personal meeting or agrees such with him/her*
> *and undertakes a concrete preparatory act to go through with the personal*

Without corresponding embodiments that can be read out in court or witnesses (parents or other children) who were present at the time of the communication, the production of evidence is thus difficult, but not impossible.

[25] Hörnle, op.cit. margin note 92

[26] Fischer, op. cit. margin note 30

> *meeting with this person, shall be sentenced to up to two years in custody.*
> *(2) Under section 1 whosoever, voluntarily and before the authority (section 151 (3)) learns of his culpability, abandons his attention and discloses his culpability to the authority, shall not be punished."*

That is doubtless to do with the fact that the offence is not known amongst the population and is therefore seldom reported, as well as with the fact that the victims – children – do not open up to parents or third parties out of shame or other reasons; it may even be the case that they consider such conversations to be normal on the Internet.

In contrast to the German offence, the Austrian legislator has not only criminalised cybergrooming, but any contact, including in the real world, for sexual purposes regarding children. Whilst the ministerial draft[27] only covered contact via forms of telecommunication and computer systems, the government bill was extended to any contact "concealing his intention". Although the introduction of this offence met with huge criticism, the obligation to implement the European Directive and the imperative to take a clear stand in terms of combatting the sexual abuse of children[28] ultimately resulted in the law being passed in the form described. What should be highlighted positively as compared to the German offence is the fact that the aforementioned problem of the "concept of written material" is solved by the blanket "use of a computer system". This formulation is contemporary and forward-looking, and it also covers further technical developments that may no longer be subsumed under the German "concept of written materials", but can be under the Austrian concept of the "computer system".

However, the Austrian offence also contains a lacuna. The offender who as an adult only conceals his age but not his intention is not covered by the offence. Yet the actual manifestations of cybergrooming[29] also involve offenders who exploit the sexual curiosity of pubescent children and openly talk about the topic of sexuality, whereby their only deceptive act is to fail to state their correct age. It remains to be seen how Austrian jurisprudence will ultimately resolve this issue.

The Austrian legislator has correctly included a further element of the actus reus in addition to initiating contact, in that it requires a "concrete preparatory act to go through with a personal meeting" with the child. However, what remains unclear is what a concrete preparatory act is in this context. In some cases there may not be so many preparatory acts for a meeting. However, it is conceivable for example that the offender needs to make his way to the meeting, e.g. buy a ticket to travel etc. However, clarification from case law is required to firm this up.

It remains to be seen what tendencies will emerge in both German and Austrian case law. Although the offence took effect as early as 2004, there is still no case law from the highest judicial instance. That is doubtless to do with the fact that the offence is not known amongst the population and is therefore seldom reported, as well as with the fact that the victims – children – do not open up to parents or third parties out of shame or other reasons; it may even be the case that they consider such conversations to be normal on the Internet. Typically incidents are only reported if the parents or third parties happen to follow the communication or if such a meeting actually takes place and comes to the attention of the parents, for example.

These issues relating to reporting behaviour can be applied to Austria in equal measure. Up to October 2012 only five criminal trials had been recorded since the introduction of the offence.[30]

[27] Cf. KU Aktuelle Kriminalpolitik 4. Einheit on section 208a StGB-Österreich

[28] KU Aktuelle Kriminalpolitik 4. Einheit on section 208a StGB-Österreich, p. 5

[29] Cf. also Rüdiger for further information

[30] Kleine Zeitung Österreich, article dated 20 October 2012

4) Problems of statistical recording

In Germany is difficult, if not impossible, to present the actual statistical scope or the statistical development of cybergrooming crimes. This is because the police's criminal statistics (at national and regional level) only record cybergrooming along with the showing of pornographic images to children. It is true that the crime often occurs in conjunction with the showing or even the creation of pornographic images. There are no notable trends within the recorded statistics over recent years, which, however, says nothing about the shifting incidence of the crimes. The distribution statistics from the national government only cover the sexual abuse of children in all legal variants. However, here too no significant increases or decreases can be identified over recent years, which means that no conclusions about the development of cybergrooming can be drawn. What needs to be taken into account is that cybergrooming under section 176 (4) (3) StGB, if it is followed by sexual acts arising from it, is subsumed by the offence of section 176 (1) StGB and therefore takes a back seat. Initiation is therefore certainly of interest as a prior incident – the background to the crime – and is often lost sight of in the police and judicial process.
To date corresponding convictions have been included neither in the commentaries or text books on criminal law nor in the "Juris" German law database.

a) Regional Court of Koblenz
The only press report, from December 2008, relates to a rape trial at the Regional Court of Koblenz. There a 53-year-old man had persuaded a 14-year-old girl in an Internet chat room to meet him at Lake Constance without her parents' permission. The 14-year-old girl did in fact travel to the agreed meeting point, where sexual acts took place, although it cannot be ruled out that these took place voluntarily. The Regional Court of Koblenz acquitted the accused of the allegation of rape, but did sentence him to one year and nine months in jail for child abduction. In the reasoning the judge stated that "when chatting the 53-year-old was solely thinking of getting young girls into bed". To do so he pretended to be younger than he is and with "great cunning" pretended to be the girl's "lover who idolised her". It used to be bad uncles who enticed children into their car with sweets, today it is the Internet that is increasingly the starting point for such serious offences, sadly including sexual ones. The unemployed man, who spent several hours a day in front of the PC, worked with "incredible imagination, almost unsurpassable tenacity and unbelievable audacity". He set up various chat nicknames such as "CuddlyBear" or "NiceGuy" and decorated his Internet profile with hearts or flowers. When the 14-year-old girl told him she was having trouble with her parents, he convinced her to move in with him and picked her up in his car."[31]

b) Berlin State Bureau of Criminal Investigation
When surveyed, the five precincts of the State Bureau of Criminal Investigation of the federal state of Berlin that deal with sex crimes estimated that there are some 20 trials per year in which the allegation of cybergrooming is tried. However, no conclusions about the actual dangers that cybergrooming poses for children could be drawn. The offence of cybergrooming, which has only been in force for nine years, is not yet as deeply embedded in the general legal awareness as other offences, some of which date back to the Ten Commandments of the Old Testament. With the intensifying discussion in the press, as well as the general phenomenon of cybercrime, and increasing preventative work in schools, a sensitisation of the population in schools and increased reporting rates can be anticipated in future. However, there is currently another practical

With the intensifying discussion in the press, as well as the general phenomenon of cybercrime, and increasing preventative work in schools, a sensitisation of the population in schools and increased reporting rates can be anticipated in future.

[31] Stern.de, article "Eingeschleimt, angemacht, verurteilt" http://www.stern.de/digital/online/urteil-zum-cyber-grooming-eingeschleimt-angemacht-verurteilt-649925.html dated 22 December 2008

he child was ashamed to tell the truth – that he/she was persuaded, and blackmailed, by a stranger into posing for photographs of child or juvenile pornography.

problem for the law enforcement agencies – cybergrooming is not even recognised. For example, a child tells a technically highly unlikely to nonsensical story about "downloading" and altering his/her photos from his/her Facebook account and sending such files to third parties. It quickly turns out that this could not possibly have occurred. But something like that! The child was ashamed to tell the truth – that he/she was persuaded, and blackmailed, by a stranger into posing for photographs of child or juvenile pornography. In practice such information from a child will prematurely cause the police to issue a transfer decree to the State Prosecutor's Office with the closing sentence "No offence". Only on a close review by sensitised investigators is such a case also worthy of proper investigation.

5) Criminal law and/or political consequences?

a. <u>Do we need statutory amendments to the German criminal law?</u>

The offence of cybergrooming in Germany pursuant to section 176 (VI) StGB penalises the corresponding conduct very widely prior to the violation of the legally protected right. The offence is already made out when a child merely takes note of the initiation.[32] A further extension of the offence that criminalises the attempt, which to date has been expressly ruled out, fails to understand the actual issues and would have no practical scope of application. The motivation of the offender alone cannot and must not be prosecuted unless there are physical consequences. Pure thought crime has no truck in our legal understanding.[33] This is also not necessary in the context of the protective purpose of the rule because by definition the legally protected rights cannot be breached by the attempted initiation.

However, the question arises as to whether cybergrooming should not be extended to the offences under section184 b – "Child pornography" – and 184 c StGB – "Juvenile pornography". In many cases the offender is not merely concerned with meeting the child, but they have the child or juvenile create pornographic images.[34] The behaviour that the offender equally tenaciously encourages in this context makes out an offence, if it is successful, (section 184 b and c StGB) and can have a significant influence on the psychological development of a child or juvenile (cf. the case of Amanda Todd).

What causes significant difficulties in practice are cases in which the age difference between the protected person and the "alleged" offender of the sexual abuse or cybergrooming is small and it appears clear to all involved that this is a "normal" sexual relationship amongst minors. However, if the sexual acts take place between a person over 14 and one under 14, the offence under section 176 StGB is made out. Both Switzerland[35] and Austria[36] have therefore introduced what is known as an age-tolerance clause. Accordingly, sexual acts involving persons under 16 (age of consent in Switzerland) are not punishable if the age gap between the participants is no more than three years. Further, in Austria a distinction is drawn between sexual acts that involve sexual intercourse and those that do not. Under section 207 (4) Austrian StGB sexual acts not involving sexual intercourse are not punishable if the age gap is no more than four years and the younger person is no younger than 12 years old. Under section 206 (4) Austrian StGB sexual acts involving sexual intercourse are not punishable if the younger person is at least 13 years old and

[32] Fischer, op. cit. margin note 31

[33] Jürgen Rath: Gesinnungsstrafrecht - Zur Kritik der Destruktion des Kriminalunrechtsbegriffs in der Rechtsprechung des Bundesgerichtshofs. Hamburg 2002, see also Prof. Dr. Marco Gehrke op. cit.

[34] Cf. contribution by Rüdiger

[35] Art. 187 (2) Swiss StGB

[36] Sections 206 (4), 207 (4) Austrian StGB

the partner is no more than three years older. Both legal wordings, which acknowledge the sexual development of young people, are options both for demarcating sexual abuse as well as cybergrooming in German criminal law.

b. Do we need stricter/longer sentences?

A connection between the length of sentence and prevention has not been proven in criminological research and is generally discounted.[37] The statutory range of sentences under section 176 (4) (3) StGB already exceeds the sentences in the Directive of the EU Council and Parliament dated 4 November 2011 (of which Art. 6 deals with grooming). That demands a maximum sentence of at least one year. The German Criminal Code sets the longest sentence at five years; in Austria it is just two years. When selecting the corresponding range of sentences, the legislator is also required to recognise the significance of the offence within the range of crimes, and also the ranges of sentences for individual crimes must be proportionately balanced within the criminal code. Thus, sexual abuse of children without physical contact – as for instance in section 176 (4) (3) StGB – must continue to attract lower sentences than that with physical contact – as for example in section 176 (1) StGB. In the cross-Europe comparison, Germany has high sentences and overall a comparatively high prosecution rate. As for the question of whether longer sentences are needed, we should not ignore the fact that many European countries impose long sentences, but start to release the convicts early on, whereas in Germany release after half of the sentence is rare and release after two thirds of the sentence is not considered in all cases.

c. Do we need different/higher ages of consent?

The age of consent refers to the age from which a person is legally considered able to consent to sexual acts. The age of consent in many countries depends on various factors, such as gender, cultural understanding etc. In German criminal law there is no uniform age of consent, but instead there are different age limits for different offences. For example, section 182 StGB stipulates that sexual acts with persons under 18 are punishable under certain circumstances specified there; under section 174 StGB sexual acts with juveniles may also be punishable if they have an educational, training or care relationship to the offender. The limit of the age of consent, here 14 years of age pursuant to section 176 (4) (3) StGB contains the statement by the German legislator that persons of this age and above are psychologically and physically capable of freely deciding over the issue of their sexuality. This statement implies – as in many areas of criminal law – a voluntative and a cognitive element (cf. section 16 StGB). If we approach the issue (higher age of consent) for the offence of cybergrooming from this perspective, we need to assess whether we trust young people of 14 and above to identify risks on the Internet, to evaluate them correctly and accordingly to take a responsible decision to protect their own sexual self-determination. In fact, we need to trust our children to do so at that age. At the age of 12 to 14 almost all children are at secondary school, they can go to school on their own, ride a bike etc. The list of what we already trust our children to do at that age could be extended further. The voluntative element therefore poses no problem in society. Although no one would let a child ride a bike if they did not know how to do so, many children of this age still lack the necessary media competence. The purely technical handling of the Internet, computers etc. can be learnt quickly and in many school is part of the syllabus from year 2 onwards, yet the specific risks and options for tackling these risks are not frequently communicated.

A connection between the length of sentence and prevention has not been proven in criminological research and is generally discounted.

[37] In place of the above: Eisenberg, Kriminologie, 6th ed. section 15

From a legal perspective the case of Amanda Todd, with the creation of the screenshots, satisfies neither the offence of cybergrooming nor of the creation or distribution of written materials containing juvenile pornography.

d. The case of Amanda Todd

Whilst this essay was being written, the media are reporting extensively about the case of the Canadian girl Amanda Todd. Amanda took her own life on 10 October 2012 at the age of 15 after years of harassment, derision and denigration via the Internet. In year seven she began to make new contacts with friends, including via the Internet. One day a cam-chat partner convinced her to show her breasts. Amanda blithely submitted to the urging of her supposed friend. This individual contacted her again and blackmailed her with naked images of her that he had produced using screenshots of the chat. When Amanda failed to respond, the man sent the images to her friends and acquaintances. Amanda became depressed and fell out with the people around her. She changed school several times and attempted suicide for the first time. In 2012 she finally took her own life.

From a legal perspective the case of Amanda Todd, with the creation of the screenshots, satisfies neither the offence of cybergrooming nor of the creation or distribution of written materials containing juvenile pornography. At best a punishable act under section 33 German Act on Copyright in Works of Art and Photography (*Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie*, KunstUrhG), which relates to denigration and derision, could be made out, although there is no further information in this regard, or perhaps an insult under section 185 StGB. It is also doubtful that the offence of negligent manslaughter pursuant to section 222 StGB is made out. The umbrella term for this "offence" is cyberbullying.

In German law there is no specific offence of cyberbullying, although individual acts may represent criminal offences. What primarily comes into question are the insult offences pursuant to sections 185 et seq. StGB, offences violating privacy under sections 201 et seq. StGB, offences against personal freedom under sections 232 et seq. StGB – in particular section 238 StGB (stalking) – and the violation of one's right to one's own image pursuant to section 22 et seq. KunstUrhG. Further, crimes such as the procurement of child and juvenile pornography pursuant to section 184b and c StGB may apply.

The German offences are on the whole well-suited to preventing attacks on these legally protected rights. At the point at which the respective laws were passed,[38] however, the intensity of the attacks was substantially lower than is afforded today by new media – for example an insult could only reach a small number of people. Nowadays the Internet means that insults can reach millions of users. The possibility of being able to anonymously vilify, ridicule and massively pressurise the victims means that the damage to legally protected rights has increased substantially. The offences are no longer in line with this development. Notwithstanding the fundamental objection that it is not often reasonable to use a tragic case to close – apparent – lacunae, offences such as insults committed via the Internet can only be punished appropriately – given their extended sphere of impact – if either a particularly severe case is inserted or the range of sentences is qualified – such as for example for the defamation of people in political life pursuant to section 188 (2) StGB.

e. Other protective measures

Alongside the specified statutory amendments, effective counteraction is ultimately also a challenge for society as a whole. Here both the legislature and the executive need to make sure that the protective umbrella of the criminal law can also be actually opened up. However, this can only be done effectively if the police and state prosecutors are given the

[38] Section 201 StGB e.g. 1967, section 185 StGB in essence as in RGStGB

staffing and technical resources to apply the legal provisions and it is ensured that officers have corresponding technical media competence.

Even when prosecuting the possession and distribution of child pornography, the police come up against limits in terms of their sometimes obsolete staffing and technical capabilities given the constantly increasing storage capacities ("big data") and new storage possibilities ("cloud"). However, in the case of cybergrooming too, PCs, laptops and other data storage media need to be confiscated and evaluated. Depending on whether there is an actual suspicion of abuse or "just" the suspicion of the possession and distribution of child pornography, as well as on the quantities of data that need to be viewed, these evaluations usually take the Berlin police between two weeks and up to three years.
It is also vital for the prosecution of cybergrooming to adapt the procedural instruments available to the police and state prosecutors to the criminalistic, criminological and technical realities. Without the introduction of constitutionally sound minimum data storage[39] demanded under European law (also known as retention of data), cybergrooming and related serious sexual offences will in many cases not be able to be investigated and punished – and consequently they will not be preventable. If the requisite procedural instruments are not made available, sentencing provisions will be exclusively symbolic. However, corresponding technical measures, such as the recording of contact details when key words are mentioned in online children's games, need to be tested and discussed.[40]

However, corresponding technical measures, such as the recording of contact details when key words are mentioned in online children's games, need to be tested and discussed.

As well as supporting the law enforcement agencies in staffing and technical terms, educational work at schools plays a key role. Children should not be expected simply to know how to use a computer and the Internet. They need to be educated about the risks and operation of publications on the Internet, which should take place at a time when they are beginning to use the Internet. This can, and increasingly will, take place in the first few years of school. Preventative programmes at schools[41] make sense, but educating the parents must also play a key part. Only if parents know what their children are doing on the Internet can they influence it.

About the authors:

Thomas Schulz-Spirohn is a state prosecutor in Berlin and the father of two children. He studied law at the Free University of Berlin between 1983-1989. On completing his practical training he worked as a research assistant at the German Federal Public Prosecutor (Bundesanwaltschaft) and then as a state prosecutor in Berlin in various general and specialist departments. Since 2002 he has worked in the department for sexual offences and publications that glorify violence, are pornographic and are harmful to young people.

Kristina Lobrecht, mother of two children, studied law at the Free University of Berlin specialising in criminology and the philosophy of law. After one-and-a-half years of practical professional experience in the area of compulsory enforcement and the handling of special tasks associated with German reunification, she completed her practical training specialising in criminal law in Berlin and took her second state examinations. She has been a District Court judge since 2011 where she specialises in narcotics law. She is also an advisor to the training and education department at the Upper Regional Court.

[39] Cf. Directive 2006/24/EG dated 15 March 2006

[40] See also the article by Prof. Dr. Lucke.

[41] E.g. in the district of Teltow-Fläming (Brandenburg)

Dutch police, vision on youth and the internet

Solange Jacobsen and Manuel Mulder

Abstract

The Dutch police has chosen to be actively in contact with young people on the internet. The underlying belief is that, for the police Youth task (prevention, signaling, advise and repression) to perform optimally, it is of crucial importance to be present in the virtual world. It is the only way to be in intensive contact with them, find out what they are doing and be there for them if they need the police.

There is a website for youngsters at www.vraaghetdepolitie.nl, twitter is used frequently, an awareness game (at www.kenjevrienden.nu) has been developed, and there is even a police officer in the virtual Habbo hotel with its own police station. There is a toolbox for police officers providing assistance and case studies on how to deal with youth (problems) and the internet. The how and why are explained by Solange Jacobsen and Manuel Mulder in this article. They sketch the current context, including the many forms of internet use and abuse, that young people face these days.

1. Digitization of society

1.1. Media use in the Netherlands

Recent research[1] indicates that 94% of households in the Netherlands have a fixed internet connection. The Netherlands is the leader in Europe, followed by Denmark, Sweden and Luxembourg (all 92%). In Europe the average is 76%. Four years ago 86% of Dutch households had internet access.

Almost 60% of Europeans use the internet daily. More than seven out of ten people go online at least once a week. The penetration of fixed internet connections is stagnating. Mobile internet on the other hand is growing exponentially. A third of Europeans between the ages 16 and 74 makes use of mobile internet. The rate among young people aged 16 to 24 is much higher: 58%.

Mobile internet growth

Recent research[2] conducted by the CBS (Dutch Central Statistical Office) also shows that mobile internet use is increasing. The number of internet users in the Netherlands in 2012 was 12.4 million, which equals 96% of all 12 to 75-year-olds. Six out of ten internet users use mobile devices. This is a threefold increase compared to 2007. Especially among young people, the use of mobile internet has increased. In 2007, 21% of young people aged 12 to 25 were online with their mobile device. In 2012, this has grown to a staggering 86%.

Growth of mobile devices

The rise of the smartphone and tablet especially has led to an increase in mobile internet use. Users maintain their contacts this way. Nearly three-quarters of them use email and almost two-thirds participate in social networks such as Hyves, Facebook and Twitter. Reading news and newspapers (62%) and playing games and listening to music (58%) are favorite pursuits, too. They do not only use mobiles devices while out and about, but also at home even when a fixed internet connection is available.

They do not only use mobiles devices while out and about, but also at home even when a fixed internet connection is available.

Four out of ten internet users do not use mobile equipment. Nearly three quarters of them (73%) indicate no need for internet outside home or work. High cost is

[1] Eurostat ,Statistics in Focus ,, week 50/2012

[2] CBS, Statline, ICT use of households and persons, October 2012

mentioned in 16% of the cases as a reason not to go online with a mobile device.

Popularity of social media

Previous research of the CBS zoomed in on the use of media. It showed that more than half (53%) of internet users in 2011 were active on social networks such as Hyves, Facebook and Twitter. Especially young people up to 25 use it a lot (88%). In addition, one in five internet users is active on the business networking site LinkedIn.

Young people are growing up with "2.0" and find it obvious that they can influence websites themselves by posting content, responding to content, receiving responses, making contacts with friends, 'friends of friends' and strangers.

1.2. Digital youth culture

In recent years various national and international studies have looked into the use of media by young people from a great number of angles. How many young people are online? How often? What do they do when they are? How do they do that? What influence has media use on their development? What influence has media use on school performance?

The common denominator in all research is very clear: media plays an ever increasing role in the daily lives of children and young people. There is more to conclude from these studies:

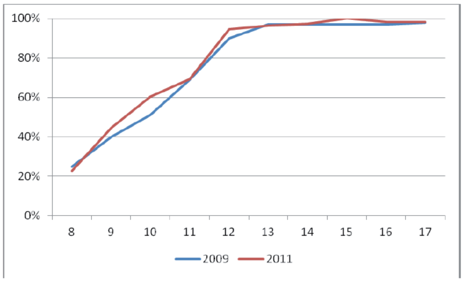
- the average age at which young people go online is dropping;
- the frequency and intensity of media use is increasing;
- there are more risks online than young people think;
- young people are less media-savvy than adults.

1.2.1. Growing up and developing with media

Young people today grow up with an overkill of media and are more "connected" than ever. They spend more time on the internet than watching television and they are constantly connected to their networks. Moreover, watching television is done through the internet at a time that suits them! With their smartphones they can, at any time and from any location, be in contact with whomever they want, gather and share information, and have fun with all conceivable forms of entertainment.

EU Kids Online Research[3] shows that 93% of 9-16-year-olds go online at least once a week and 60% do it (almost) daily. Age is a strong determining factor; the older, the more intensive. Of the 9 to 10-year-olds who use the internet, 30% are online daily. Of all 15-16-year-old internet users the figure is 80%. The average age at which children start actively using the internet for the first time is seven years.

The transition from primary education to secondary education seems a natural time for children to get their own mobile phone. The table below from the study "Hey, what's app?"[4] about the possession and use of cell phones shows that 75% of all 9-11-year-olds have their own phone. From 12 years, this figure rises to 98%.



Source: Mijn Kind Online "Hey, what's app?"

Decide "what, when and how"

Young people are growing up with "2.0" and find it obvious that they can influence websites themselves by posting content, responding to content, receiving responses, making contacts with friends, 'friends of friends' and strangers. Hidden behind vague profile pictures or avatars they exercise social skills, push their limits, build self-confidence and experience what

[3] Haddon, Leslie and Livingstone, Sonia (2012) EU Kids Online: national perspectives.EU Kids Online, The London School of Economics and Political Science, London, UK. Version available at: http://eprints.lse.ac.uk/46878/

[4] Foundation my child Online, Hey, what's app?, March 2012

suits them and what not. Young people discover their own identity this way. Quick interaction is pivotal and young people want to decide how and when they do something; using What’s app, making calls, chat or write online messages via Facebook and Twitter. Sometimes they do it using the home computer, at other times, such as on the train, by using their mobile phone. They leave environments very quickly that do not comply with their needs. They don’t want to wait long for replies or responses.

Being creative with language

As a way of communicating, young people have created their own new forms of language. MSN language (or chat language) and sms language are the best known. Chatting speed is essential here. The use of emoticons (☺) and the use of numerals instead of letters (w8 instead of wait) have their origin here. Abbreviations such as BFF ("Best Friends Forever"), and YOLO ("You Only Live Once") are widely used.

Go online or being online?

Many adults who access the internet see the internet as a virtual world where they can find information and where they can do business. They ‘*go online* ‘ to attend to their banking affairs, to find a holiday or to order something. On the other hand, young people ‘*are* online ‘... They are simply doing the things they do and use the technologies available to them. For them there is no difference. Online = offline...!

Ten years ago the internet was mainly a gigantic library. Nowadays, it can be compared with a meeting center that is open all day and night and offers many possibilities for service and entertainment. The fact that the internet is the underlying infrastructure that makes all of this possible is irrelevant, especially for young people. For them it›s simple: you can get in touch with friends and be a part of a larger community. It is an essential part for growing up, which includes the development of social skills and finding your own identity. That happens nowadays for a large part online. Contact with classmates is not limited to the schoolyard or school hours. Via social media and what's app they are connected 24/7, to the great frustration of teachers and other adults. They worry about this 'face-down generation' who only seem to have an eye for smartphones or tablets and are distracted from homework and 'real' contacts.

Nevertheless, this generation is not actually any different to their parents. They have the same need for connection and they adapt to belong to a group. The significant difference, however, is that schoolyard dynamics does not stop anymore. Not participating is not a real option. If you don't participate, you are no longer a member of the group. Do you want to stand alone in the schoolyard?

When it comes to finding their own identity, young people today have exactly the same questions as their parents had: 'who am I?', 'who do I want to be?', 'what suits me?' and 'what doesn’t?'. And they also find the answer, like their parents, through contact with others. But, of course, the internet offers many more possibilities for this and thus plays an important role. You can present yourself on profile sites with photos and videos that you upload. In chat sessions, whether or not you use a webcam, you can practice your social skills. The way the interaction proceeds is crucial for the image that teenagers have of themselves. Who am I, what do others think of me, am I 'good' or ‘cool’, what are my hopes and expectations and what do I want from life. Sometimes the internet is the place to be in touch with people who share your passion, or your orientation. Flirting and experimenting with sexuality has expanded to include not just the schoolyard, the hangout, the pub and nightclub, but also the internet.

In chat sessions, whether or not you use a webcam, you can practice your social skills. The way the interaction proceeds is crucial for the image that teenagers have of themselves.

Generation Einstein?

Give a toddler a smartphone or tablet and he will soon find out how to create larger or smaller images. He learns this by doing, seeing and he remembers. Children are not afraid to discover something new and learn that way how new technology works very quickly (aided by the fact that new technology is increasingly more intuitive).

Because of this adults may believe that they cannot teach anything to young people anymore. That is not true. The fact that children can adapt quickly to new technology does not mean that they understand everything, appreciate the consequences or know how to deal with them. This is certainly not the case if they are confronted with age-inappropriate information or footage. Young people between 12 and 18 prove[5] less able than is often thought. They make a lot of mistakes because they are impatient and bad readers. They are also naive and not very critical. Research by Dialogic[6] shows that 80% of high school youngsters don't check the reliability of the sources they use. It also showed that "finding privacy as important" is not the same as "knowing what to do to protect ones privacy" or "to act correspondingly".

Young people between 12 and 18 prove less able than is often thought. They make a lot of mistakes because they are impatient and bad readers. They are also naive and not very critical.

Young people know in theory what is wise and/or safe. But searching and pushing the boundaries is exciting and is inevitably linked to growing up. During the moment, doing something comes before thinking. They simply don't see the consequences of their behavior; YOLO ...!

1.2.2. Where are they?

A frequently asked and investigated question is what is popular among young people on the internet; What do they like? Which sites do they visit the most? What internet application is their favorite? YouTube, the website where users can post videos and that everyone can use to watch movies is by far the most popular in all age categories. Young children watch fun movies on 'Joeptjoep' together with their parents

Finding answers to such question as 'where are they ' and 'how long for', however, is of little value for understanding digital youth culture. It is far more important to know how websites and applications facilitate and support the development of young people.

For young people social network sites are important for a number of reasons:

- **Being in contact.** The need to share, join a group and oppose adults is part of growing up. Online you can do this continuously. The fear of adults that social networking sites replace 'real' friendships and that young people become more antisocial is unjustified. They just amplify it ...
- **Comparing yourself to others.** For young people it is important to compare themselves with others. What do others look like? What do they wear? What music do they like? What do they do? Social networking sites are an excellent way to 'peep' unabashedly at what others do. It helps young people to determine their own identity.
- **Presenting yourself.** If you look at other people's sites and profiles you know that others also come to visit yours. Young people therefore give endless attention to their online profile. They choose the best picture, the funniest texts, the right movie and the hippest music. At Hyves young people can also indicate what brands they want to be associated with. The success of sites such as Facebook and Hyves depends entirely on the fact that young people are constantly concerned with the question how they are seen by others. The fact that they themselves have control over how they present themselves gives young people

[5] my child Online, Research Foundation "Einstein does not exist", October 2010

[6] Dialogic, research "behind the scenes: Media use and behavior vmbo-youth", November 2012

a feeling of being better and stronger. Even when you're not the most popular person in the classroom, a strong profile on a social networking site gives you the chance to distinguish yourself in a positive way.

- **Receiving feedback.** The internet is all about action and reaction. Young people watch each other closely and are on standby to give a (usually positive) reaction to pass on messages and photos. The attention and compliments contribute to the group's feeling and to self-confidence.
- **Making contact.** Social network sites are easily accessible; it is very easy to make contact with 'vague acquaintances', including people from their wider circle of friends and acquaintances. Here you can leave a message (a Scribble) whenever and for whoever you want.

Computer games are as old as the first computer. The game Pacman had it all. It was fun, exciting and very addictive. Most games stimulate creative ability through playing. Young people learn to negotiate, practice solution-oriented thinking and their social skills. Even for the little ones there are games that suit their age.

Internet games have evolved into what they are today: beautiful, realistic and often complex games with an infinite number of variations and possibilities. You can play alone or online with others around the world. By any means whatsoever: computer, smartphone, iPod, tablet, handheld game consoles (such as Nintendo DS) and game consoles for television (Xbox, Wii, Kinect). Online games are very attractive. You play with others, get instant rewards for assignments that you perform and receive appreciation from the other players.

1.2.3. Online risks

The internet clearly offers young people a world with a lot of possibilities and opportunities, but also risks they are not, or insufficiently, aware of. The internet is anonymous and takes away inhibitions. This means that 'ordinary' norms and values are shifting on the internet. Boundaries are not always very clear and youngsters are already pushing the limits by looking for their own boundaries and by having quite a different perception of the use of the internet.

Research shows that young people from 12 to 18 make massive use of the possibilities the internet offers for romance and erotic encounters. Most adults have no idea that almost all young people who are active on the internet have been sexually approached by someone, or that one in four boys and one in five girls have had some kind of online 'sex' experience.

The internet clearly offers young people a world with a lot of possibilities and opportunities, but also risks they are not, or insufficiently, aware of.

Sometimes 'internet friends' have other intentions and can be very annoying. Young people see that risk much less and sometimes not at all. They just give out personal information, make appointments or expose themselves literally in front of the webcam, with all sorts of consequences. Usually they resolve it themselves, whether or not with the help of friends, parents or the school. But it also requires action from the police when criminal conduct is involved.

Sexting

Sexting is sending sexually suggestive messages or spicy photos or videos, usually via a mobile phone. "Sexting" consists of the English words "sex" and "texting". Both adults and young people find this exciting to do with their friend or girlfriend. It is increasingly becoming part of a sexual relationship. For young people it is logical to experiment with media such as mobile phone or webcam as part of their sexual development.

Sexting, however, is not without risk. The consequences can be far-reaching if the images are put online by an angry ex to take revenge. Sexting however is not always voluntary. Victims can be manipulated, blackmailed or threatened to send a nude photo. Once they have done it, the offender threatens to put the photo on the internet or to distribute it in some other way. Victims are then forced to engage in further sexual acts, for example, through the webcam or even in real life.

According to current Dutch legislation sexting is punishable for youngsters under 18. It's punishable by law to create, possess or disseminate child pornography. The law itself doesn't take sexual experimenting by teenagers into consideration, but fortunately the administration of Justice does.

Webcam sex (abuse)

Most young people think it's fun to flirt and experiment with sexual behavior on the internet. They generally can also deal well with unpleasant experiences. But there are also victims and losers. Especially girls find it sometimes difficult to refuse things, forcing them go further than they actually would like to. In some cases, webcam sex images are published online; out of revenge after a broken relationship or in the form of cyber harassment. The same as mentioned for sexting applies here. The damage that this can cause is great; it is even possible for the images to continue to haunt the victim all her life, often without the offender even realizing this when performing such an impulsive act.

Under threat of disclosure of recorded images young people are pressured to go much further in front of the webcam or even to meet for physical sex.

The risk of abuse is very real and the impact, when this is the case, immense. Under threat of disclosure of recorded images young people are pressured to go much further in front of the webcam or even to meet for physical sex. This is also a way lover boys operate and leverage young people's loyalty.

Fake scouts

There are fake scouts that pretend to be scouts for a modeling agency or photo studio who shower young people with compliments and promises and take advantage of people's lack of self-esteem and their need for positive confirmation. They continue until these children sign up and pay the so-called photo studios and modeling agencies. In addition to the financial abuse (scam), sexual abuse is also just around the corner.

Unwanted publication

Photos or videos of yourself that you prefer not to share with the whole world can appear online; drunk, naked, crazy faces, in your bikini at the new year's party. It happens regularly that images without the consent of the 'protagonist' are put on the internet by someone else. This can be done as a reminder of a nice evening or just for fun because he or she does not understand why the other person would have a problem with it. Sometimes it happens with the express purpose of bullying, as revenge or with the conscious intention to annoy the other person. Given the enormous growth of social media, the threshold to publish is low and the impact is often great.

Insult, Slander/Libel

The internet offers many ways to hurt someone's good name and honor. For example, by creating a video of edited (profile) photos and making it clear through text or lyrics that the protagonist is a whore. Or by spreading a so-called 'Banga-list'. This is a list of girls by name, supplemented by personal data, (profile) photos and an explanation why they are among the top X 'largest sluts' of the school, city or province. Young people are very creative with finding new ways to do this and may go far. Other examples are:

- creating a hate profile with edited photos
- emailing edited photos
- putting offensive lyrics on forums under the name of another person
- putting some person's name or photo next to offensive lyrics

Virtual theft

A common form of theft takes place in (paid) online games: the looting of rooms in the virtual game Habbo, where players have paid for the decoration of rooms and therefore this represents value. Robbery on the internet is of course different from robbery at home or in the street. By obtaining passwords or codes you can login to someone's account and 'become' that person's online identity. You then have free access to the game and his or her virtual property which you can book to other accounts. User data can be obtained in different ways. They are:

- told in confidence (best friends have no secrets)
- collected through so-called. 'phishing'
- simply guessed by obvious name and password
- obtained by threat

Cyber bullying

The tendency to find one's own limits can hurt other youngsters. Teens have a different view on bullying than adults. In the eyes of many young people bullying has a high fun factor and you are a tough guy when you go to the edge, and beyond. Bullying on the internet is anonymous and easy. A bad message is sent within a heart beat. What they don't realize, or what just doesn't interest them, is that what happens on the internet will not simply disappear again and can even become criminal.

Online bullying has a much bigger impact than classic bullying because as a victim you are not safe anywhere anymore. The bullying continues even if you're at home. It is invisible to parents and teachers and can continue for a very long time because victims do not dare to tell for fear that the bullying will get worse. When online bullying is recognized, in general it's dealt with by parents and the school. Not only do youngsters cross limits easily, they often are victims of cyber bullying themselves. Research shows that often there is a relationship between offline and online bullying. Cyber bullying is, like bullying, in itself is not punishable, but it can certainly contain criminal elements.

The bullying continues even if you're at home. It is invisible to parents and teachers and can continue for a very long time because victims do not dare to tell for fear that the bullying will get worse.

Minimizing risks starts with your own behavior

Many of these risks can be minimized by making young people aware that they themselves have a responsibility and by teaching them how they can protect themselves. Herein lies an important role for parents, educators and teachers. But also operators of online environments can minimize the risks and take measures to provide a secure environment to young people. In the Netherlands a lot has already been done in this area.

European research[7] into the use of media by young people places Dutch youngster (just like young people from Cyprus, Finland, Poland, Slovenia and England) in the category **'Higher use, some risk'**. Despite the fact that they are intensive users of media, they are less likely to become the victim of online risks than young people in other European countries. As a possible reason for this increased resilience is mentioned:

- effective awareness campaigns
- active involvement of parents in their children's use of the internet

1.3. The online domain

Taking a helicopter view of all the facts and figures in the preceding paragraphs it becomes obvious that with the advent of the internet and all its applications a new social environment has been created where (young) citizens spend time, make contact, make money, can commit criminal offences and therefore can be victims. In this document we use the following description for the online domain:

"the total of all online environments and applications through which contact between people and the resources they use for it is possible".

[7] Haddon, Leslie and Livingstone, Sonia (2012) EU Kids Online: national perspectives.EU Kids Online, The London School of Economics and Political Science, London, UK. Version available at: http://eprints.lse.ac.uk/46878/

Characteristics of the online domain

1. Not tangible

The contacts and interactions take place in the “internet cloud”. You can’t look people in the face, put handcuffs on them and haul them off for example. The presence of the police in the virtual world requires us to consider in depth how you can display confidence and exercise authority.

It is a challenge for every organization that is geographically organized to find an efficient and effective solution to existing processes.

2. Boundless

The internet has no borders. People contact each other all over the world. Offenders and victims of internet abuse may live kilometers apart. Moreover, it is not inconceivable for the many victims of one offender to all reside in different geographical areas. It is a challenge for every organization that is geographically organized to find an efficient and effective solution to existing processes.

3. No public space

Everyone surfs freely and without restrictions on the internet. Contrary to what you might think (certainly about the term “world wide web”), you cannot compare it with a public space. The internet is a network of computer networks on which all kinds of services are offered. Every website or online environment is therefore the property of a company or private person. The internet is a concentration of private spaces where the owner sets the rules (terms and conditions!). This is a very important factor in determining the size and content of the task of the police in the virtual world.

4. Information all over

The present situation, in which you can ‘listen’ as an outsider to conversations between people, look at their photo album and have access to personal information, is unique. There is a lot of publicly accessible information around through the use of social media : what keeps people busy, where they go, who their friends are, who their family is, what hobbies they have, and what they have experienced and seen.

5. Privacy

The issue of privacy in the online domain is associated with additional complexity. Most citizens seem not overly worried about the issue of privacy because they think ‘I have nothing to hide ‘. They publish information about themselves on a public profile without realizing the range or possible consequences. Only when they are confronted with ? do they become obsessive about their privacy. Equally the question ‘what do third parties do with information once published’ doesn’t matter to many citizens. For the police this presents opportunities; public profiles are still seen as public sources, provided that information is not systematically collected.

6. Nothing is what it seems

The internet is anonymous. People hide behind (a homemade) profile and use nicknames and Hotmail addresses. Data can be manipulated on the internet, so you should always be critical and ask yourself: “What is true?”, “Can I trust this person?” This is not always easy; a rumor on the internet quickly turns into the “truth”. After all, if so many people talk about it, there must be a kernel of truth in it!? And when there are even pictures to support it, then all doubt quickly disappears and only a few people are left who wonder whether the image may perhaps have been manipulated.

7. Dynamic

How quickly communication travels these days and what impact communication can have is illustrated by the various experiences from the 2012 projects X. There are, however, also numerous examples that illustrate how quick ‘smaller’ items of communication travel nowadays. The first photos of an accident, for example, are sent by twitter within a few minutes (sometimes even before a police control room was informed about the accident), and regularly a tweet proves to be the actual source for reporting in the national media. Today everyone is a producer of news and dissemination is faster and better targeted than in any other medium.

The above examples focus on the differences between the online environment and the 'physical' environment that we know. However, there are also a number of similarities between the two environments that are important to bear in mind for further reflection on the role of the police in this domain:

1. It involves real people, really money and genuinely criminal behavior
2. Legislation in respect of minors (special position, both criminal and civil)
3. Expectations of citizens towards the police to be "watchful and helpful"
4. Preventing, identifying and advising are important factors for preventing an escalation
5. Certain situations require (emergency) assistance
6. Cooperation between organizations is essential

The online domain generates challenging issues when it comes to translating them into the core processes of the police and the implementation of the tasks of the police and more specifically the police youth task.

1.4. Online victims and offenders

With the advent of the internet, new forms of crime have emerged. Crime that does not exist without the necessary IT facilities (computer and/or network). We speak of 'cybercrime in the strict sense'. Examples are:

- Hacking (accessing data on computers without permission)
- Defacing (changing, replacing, or destroying data from a website without permission)
- Spreading malware (malicious software that damages computers and network connections and/or gives access to the computer or data to another person without the consent of the user).

In addition, there is also "cybercrime in the broad sense". This concerns criminal behavior in which IT plays a role, but is not a necessary condition for the crime itself. It applies to all offences in the criminal code, but in a new form. Some examples:

Theft: *"all my furniture in Habbo is gone!"*
Threat: *"@anyorganization I will kill you all tomorrow #deaththreats"*
Libel/slander: *"Help, I'm placed on a banga list" (girls names on list, called a whore)*
Various*: *"the whole school has seen my nude photo. First only on what's app, but now also on twitter"*

* in the case of the distribution of a nude photo there can be several relevant legislative measures. Child pornography (if the victim is a minor), grooming (if the offender is an adult), libel/slander, portrait rights, sexual abuse (if not entered into voluntarily). The context is essential for determining which offence we are dealing with.

The more users understand how the Internet works and what the consequences of their actions are, the more aware they will be with regard to their own behavior and that of their environment.

The basis for the prevention of internet-related crime for a large part lies with the awareness of the users. The more users understand how the Internet works and what the consequences of their actions are, the more aware they will be with regard to their own behavior and that of their environment. The basis of media wisdom is:

- knowing what the opportunities and risks of the internet (applications) are
- understanding the impact of your own behavior and actions on the internet
- understanding what you can do yourself to minimize risks and prevent victimization
- being able to apply this knowledge for using media responsibly and consciously

1.5. Stakeholders

Security is a collective responsibility in the virtual world!
Countering blurring of moral standards and lowering the number of criminal offences in the online domain is a task that the police cannot perform alone and should not have

to do alone. Creating a safe environment for young people on the internet is (should be) a shared responsibility of many parties. Below you find a list of parties which are relevant in addition to the police for increasing security in the virtual world.

Young people, parents and schools

An important responsibility, of course, remains with the young people themselves. When they are aware of the risks, their own behavior and its consequences, the risk of victimization is reduced. They will be self-reliant and recognize possible abuse earlier; this knowledge will also be actively used to protect yourself and others in your social network.

It is important that parents support their children in discovering the virtual world. Education determines to a large extent the standards and values of young people. This is no different when it comes to using media. It is for a large part about social skills. Depending on the age of their children parents will accompany their media use and learn how they can use this in a positive way. It also requires that they make children aware of the risks and teach them how to protect themselves: with rules and by reflecting on their own behavior. Schools also play an important role in teaching values and raising awareness to young people. They also have an important function when it comes to early signaling of unpleasant situations.

An important responsibility, of course, remains with the young people themselves. When they are aware of the risks, their own behavior and its consequences, the risk of victimization is reduced.

Owners/administrators (providers)

The responsibility for a safe environment lies to a large extent with the owner and/or operator of a site. He is primarily responsible for rules and the monitoring of compliance. Possible measures include:

- house rules and imposed conditions on the use of/visit to the online environment
- moderators overseeing compliance with house rules and taking measures in case of infringement
- providing the option for young people to contact the moderator to report misdemeanors
- prevention through technical restrictions (language filters)
- providing information on safety for young people and parents

Private parties

Several large and smaller initiatives focus on information and assistance, such as the (online) de Kindertelefoon, Meldpunt Kinderporno op Internet, Meldpunt Discriminatie, Slachtofferhulp, Bullyweb, Stoploverboys.nu, Pestweb etc.

Centers of expertise „Youth and Media“

In the area of security for young people in the virtual world various parties engage with the question "how is the digital youth culture developing" and what is needed to increase awareness and safety.

Internet Security Platform

The platform consists of several market stakeholders, the Ministries of Economic Affairs and Justice, and it aims at a structural contribution to improve internet safety for consumers/internet users. It focuses on strategic issues in relation to internet security and aims to set an agenda, identify trends and suggest concrete initiatives.

2. Impact on the police

The digitalization of society is a development that affects the entire police organization and all of its core processes. Not only because of the fact that citizens want to be able to make reports online, and expect the internet to be used efficiently and effectively in matters of detection. But above all, because the police has a responsibility when it comes to criminal behavior that is committed using the internet. The physical world is no longer the only environment in which people can commit criminal offences and therefore also be victims. Insight into the digital youth culture offers an integral perspective for wider issues and organizational challenges that the police faces:

- 'New' criminal offences
- Other forms of existing criminal offences
- New forms of knowledge about crime and legal system
- Using the internet as a new channel (communication, detection, service for citizens)
- No insight into new trends and developments
- Heavily reduced level of information without a focus on online domain
- Risk of incorrect assessment of powers through a lack of knowledge
- Inefficient business processes and chain cooperation
- Growing gap between online crime and likelihood of detection
- Less respect and trust from citizens

Young people indicated that if they need the police, they cannot find them in the online domain. To contact the police they generally have to go to a physical police station. The threshold for young people to get in touch with the police about what they experience online is great. This has several reasons:

- shame; they dare not talk about the immediate cause
- fear of not being taken seriously by the police;
- fear that the police will not understand them;
- perception that nothing happens with their report
- don’t want their parents to be involved;
- lack of direct (online) contact options is discouraging

It has therefore been decided to take the challenge and (literally to an extent!) move into the virtual world. The Dutch police has launched various initiatives in recent years in order both to learn and to use this newfound knowledge for finding answers to the organisational challenges they face. Many meaningful steps have been taken. In the following paragraphs a brief overview on the role of the police on the internet will be discussed.

2.1 Police in the virtual world

Citizens’ expectations for the police to act no differently online than in real life was an important starting point for developing and conducting the various initiatives as these expectations are legitimate. The police should be there when they are needed, help victims and arrest perpetrators. However, there are a number of constraints on the way responsibilities can be performed in the online domain. The police on the internet cannot:

- be responsible for the public order; they are private domains,
- directly apply its powers; quite often it requires special investigative techniques,
- exercise the same authority as on the street because of visibility, recognition and limitation in applying its powers,
- be the only one responsible for the safety of young people.

Young people indicated that if they need the police, they cannot find them in the online domain. To contact the police they generally have to go to a physical police station.

1. Police officer on Habbo

Within the virtual Habbo world the police has experimented with a digital community police officer, Boudewijn Mayeur. Young people can get in touch with him while playing online in Habbo. They ask a lot of questions and also confide in him about serious personal problems such as domestic violence and sexual abuse. They also regularly show him new phenomena and inform him when they are being approached for webcam sex (cyber grooming).

The reason the Dutch police started this initiative in Habbo Netherlands in 2010 was because both the community manager and the Habbo users themselves said to need the presence of the police. It started with monthly consultations for young people in what was called ‘the information-bus’ at Habbo Hotel, where other organizations like Child phone, Bullyweb, Help-wanted and Stop loverboys also were regularly online for one hour chats with the kids.

It turned out that the request from youngsters was not only to talk about the problems that took place within Habbo itself, but also about situations that happened to them outside, in the real world. They were anxious to talk with a real police officer online in their own trusted environment. Habbo created a special police-avatar and to make clear that this is the only real police officer in Habbo, a special police badge was designed. And in autumn 2012 even a virtual police station was opened.

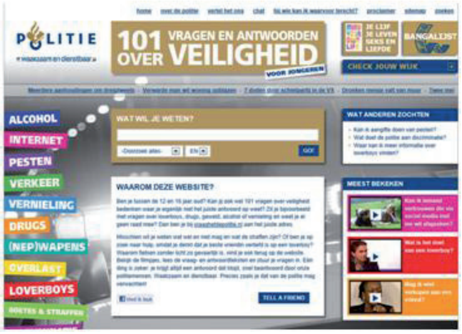
Habbo created a special police-avatar and to make clear that this is the only real police officer in Habbo, a special police badge was designed.

By being present in Habbo the police fulfills the objective to be available online to young people and thus also directly meets its responsibilities of prevention, enforcement, detection and signaling. Visibility and presence in particular are important conditions as those provide an easy contact opportunity between these young people and the police. It helps the police to better understand the experiences of young people regarding current (online) issues. On top of that they gather useful experience when chatting with young people and learn how young people value the possibility to have contact with the police online.

Last year the digital police officer worked for more than 150 hours in Habbo during 350 sessions. Over the course of 6 months there were nearly 11,000 unique Habbo users who visited the police station. Online young people are willing to provide the police with information, either upon prompting or voluntarily, about unwanted and/or harmful behavior that they have experienced. Almost every session provides us with indications for detection or further research. Because it is impossible for one officer to research all this information in the pilot phase decision was to only perform advisory and signaling work. Very serious matters were immediately passed on to colleagues in the country with the request to take over the investigation. The ambition is to extend police capacity.

2. Website Vraaghetdepolitie.nl (ask-the-police)

In addition to the existing general site of the Dutch police www.politie.nl there is a separate one for young people, which was launched in 2006. The site www.vraaghetdepolitie.nl was developed to answer questions and provide easily accessible information on topics young people themselves chose as relevant. The purpose of the website is to improve the image of the police among young people (12-16) and reach the target group that actively becomes involved in security issues in their own environment.



The presence of the website is an important step for the police in increasing their visibility and accessibility for young people in the virtual world as it enables online contact between police and young people. Young people can ask their questions, look up information, get in contact with their local police officer, take part in regular chat sessions. In the process of developing the site research was done among young people about what they expect from the police and what topics are most relevant for them. They answered that they see the police especially as an authority and wanted to find reliable factual information about topics that concern them as well as tips on how to deal with problems in this area. They also wanted to find information about laws and rules and how to contact the police. Based on this research 14 topics were chosen, such as internet, cyber bullying and drugs.

Frequently asked questions (FAQ) and answers are available for everyone to see and anyone can join chat sessions if they want. The chats topics are either themes communicated in advance or issues related to current news. The site is a huge success and at the time of writing there are approximately 70,000 unique monthly visitors to the site. Incidentally, local police officers themselves also use this site to find the answers to the questions that they were asked by young people in their district on the street.

The website is actively affiliated with a number of governmental and private bodies to allow young people to directly ask for help when they find themselves in a difficult situation online. The website www.meldknop.nl (report!) was launched on Safer Internet Day, on 6 February 2012, by the Minister of Safety & Justice, Mr Ivo Opstelten.

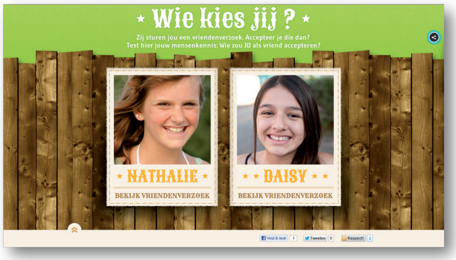
3. Communicate via Twitter

Twitter is becoming increasingly popular and virtually all sworn police officers already have (or very soon will be in the possession of) a mobile phone that allows them to search police databases themselves, but also to use Twitter independently to send short messages about their work and to inform the public or ask them for assistance. More than 1000 Twitter accounts actively communicate about police and regional matters. Before the officers start twittering they attend a short training course about what does and doesn't fit in the communication policy and share experiences and lessons learned.

4. Information about online risks

To reduce online victimization information is needed. It is for this reason that an information and awareness-raising process was developed in the form of a short "game". This game about choosing what friends to accept is called www.kenjevrienden.nu and can be played and shared with friends throughout the internet and social media. It illustrates that on the internet everyone can pretend to be anyone. The message is that it is good to think twice about who you add to your online network(s).

We know from conversations with young people that there is a high threshold to go to the police when they have got into trouble online.



★ Wie kies jij ? ★

Zij sturen jou een vriendenverzoek. Accepteer je die dan?
Test hier jouw mensenkennis: Wie zou JD als vriend accepteren?

The concept was developed together with young people and is based on true facts. We know from conversations with young people that there is a high threshold to go to the police when they have got into trouble online. Often they are ashamed and think they are not entitled to help. An additional reason is that they think that the police still don't understand what they play online and therefore their problem will not been taken seriously. With this 'game', we want to reduce the threshold for young people by showing that the police does understand what is going on online, how you can become a victim while you are online and that we understand that it is difficult to talk about it.

5. Increase knowledge level

It is important that every policeman and woman understands how online and offline are interwoven and that there are situations that require police action. To this end, various initiatives were taken, such as the production of a brochure (online) in cooperation with a center of expertise in the field of 'children and the media' about digital youth culture and its impact on the police.

It is important that every policeman and woman understands how online and offline are interwoven and that there are situations that require police action.

Furthermore, various workshops were organized on the subject of youth culture and the internet and a toolbox is designed for every colleague who, in their daily work, encounters the subject "youth & the virtual world". With the introduction of the toolbox the digikids expert group also wanted:

- to promote exchange of specific knowledge,
- give insight into local and regional initiatives,
- make proven successes available,
- to encourage cooperation.

The toolbox is not static, but constantly under development and the content grows 'with' current developments.

3. Our ambition

The ambition is to carry out an active policy on the youth task (prevention, signaling & advise and repression) in the online domain. This means reduction of online victimization and increasing the chances of arresting online offenders. Activities are designed to contribute to being present online, to be approachable and to identify what's happening at an early stage and to be able to anticipate matters. The skills of employees will have to include understanding online risks and the underlying mechanisms so that this can be translated into desirable and/or required police actions. Active knowledge sharing and cooperation with external stakeholders in the area of online safety is one of the basic conditions.

Source Entry

Eurostat, 'Statistics in Focus', week 50/2012

CBS, Statline, ICT gebruik van huishoudens en personen, oktober 2012

Marketingfacts, 'What's happening online?', juni 2012

EU Kids Online: national perspectives. Haddon, Leslie and Livingstone, Sonia (2012)

Stichting Mijn Kind Online, Hey, what's app?, maart 2012

Stichting Mijn Kind Online, onderzoek "Einstein bestaat niet", oktober 2010

Dialogic, onderzoek "Achter de schermen: Mediagebruik en –gedrag vmbo-jongeren, november 2012

Oriënterende gesprekken met Habbo, Hyves en Meldpunt Kinderporno

Onderzoek Universiteit Twente "Grooming, Sexting en Virtuele diefstal; VMBO-Jongeren en praktijkexpert aan het woord", december 2012

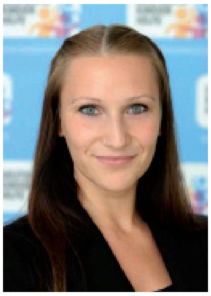
Beleidsadvies Expertgroep Digikids "Het organiseren van de politiële jeugdtaak in de virtuele wereld", januari 2013

Authors

Solange Jacobsen is an independent project manager associated with the Foundation Mijn Kind Online (My Child Online) and works for the Dutch police as program manager of the expert group Digikids.

Manuel Mulder (MBA) is a Dutch police commissioner and chairman of the expert group Digikids whose responsibility it is to develop initiatives on the subject of "reducing online risks for children" and "increasing the chance of getting caught".

Protection of children and young people in the face of the challenges of Web 2.0



Ines Kawgan-Kagan, M.A.

Abstract

The tasks facing German child protection in the media are complex and constantly need to adapt to new aspects of the Internet. The legal position in Germany, however, is even more complex. Various laws have been simply amended in line with changes on the market. Unfortunately, this has obscured the view of the whole picture and many aspects of child protection in the media are governed differently by an array of laws. Particular mention should be made of the German Protection of Young Persons Act (Jugendschutzgesetz, JuSchG), which applies to computer games, the Interstate Treaty on Child Protection in the Media (Jugendmediaschutz-Staatsvertrag, JMStV), which creates a framework for telemedia services and content, as well as the German Criminal Code (Strafgesetzbuch, StGB). We need a paradigm shift that includes a uniform and preferably international solution of regulated self-regulation for computer games and other telemedia content and services as well as an extension of the criteria for the age classification of such content and services. The sensitisation and education of children and young people, parents and teachers to the relevant issues is also crucial.

The Internet is without a doubt one of the most hotly debated innovations of the modern age; yet it is now hard to imagine life without it.

1. Introduction

"For this discovery of yours will create forgetfulness in the learners' souls, because they will not use their memories; they will trust to the external written characters and not remember of themselves."
(Plato, Phaedrus)

"Screen-based media drastically diminish the ability of children and young people to learn. The consequences are deficiencies in literacy and attentiveness, anxiety and desensitisation, sleeplessness and depression, obesity, violent tendencies and social decline."
(Spitzer, 2012)

There are 2,400 years between these quotes. A brain researcher is currently warning against the consequences of digital dementia, just as Plato did long ago, who also feared dementia caused by the introduction of writing – though this obviously turned out to be a success story. It is interesting that many people clearly have difficulties in seeing the opportunities in the unknown and unfamiliar instead of just the risks and dangers. When the first railways were introduced at the beginning of the 19th century, even doctors warned against incalculable effects of the high speeds on the brain (Joerges, 1996).

The Internet is without a doubt one of the most hotly debated innovations of the modern age; yet it is now hard to imagine life without it. Many parents see a ban as the only way of protecting their children. However, to stand in the way of progress is neither possible nor reasonable and children and young people cannot be completely shielded from the digital world.

2. Background

Completely prohibiting children and young people from using the Internet and new media is frankly unfeasible as, from a certain age onwards, parents can no longer follow their children's every move and free space is important for development. Further, in the age of mobile devices, there are no clear limits to parental authority. Healthy development depends on us experiencing things for ourselves. This does not mean leaving the younger generation to its own devices, but rather imparting important rules of conduct to them that they can use. Unfortunately, many parents are not aware just how intensively children and young people already use the Internet. Statistics show an ever younger audience using these increasingly frequently. According to the latest KIM (children and media) study, 57% of German children between 6 and 13 have at least occasional experience of the Internet (KIM study, 2011). For two thirds of children the main focus is on keeping in touch with friends. (Schröder, 2012). Yet online games are also a popular pastime on the Internet. This form of Internet use is largely unsupervised: according to a cross-Europe study, just a third of parents use a filter, and even fewer (27%) use monitoring software. The same study reveals that around 80% of parents worry about their children using the Internet. According to another study, the number of users of child protection programs in Germany is even lower at 20% (Hasebrink, 2011), although 95% consider such software to be important. Such discrepancies can be also be explained by a certain feeling of helplessness on the part of the parents. Many simply do not know how to protect their children effectively and what programs afford adequate protection.

This form of Internet use is largely unsupervised: according to a cross-Europe study, just a third of parents use a filter, and even fewer (27%) use monitoring software.

One of the best-known problems is how to handle private data and the privacy settings on social networks such as Facebook or Myspace. Only 43% of 9 to16-year-olds across Europe use the protection of setting their profile to not public; more than a quarter have no protection whatsoever and have set up a publicly-accessible profile (Haddon et al., 2011). What problems are caused by increased usage behaviour?

Common problems are online addiction and cyberbullying. Almost a fifth of 12 to 17-year-olds across Europe, making up more than 4.5 million children and young people, state that they have been victims of cyberbullying (National survey of American attitudes on substance abuse XVI: teens and parents). A key factor here is the length of daily use: the longer social networks are used, the higher the probability of becoming a victim of cyberbullying. Whilst just 3% of children and young people who do not use social networks most days are affected, the probability increases to 33% for those who spend more than an hour online.

A further problem is online addiction, and there is a link between this form of addiction and the abuse of other substances such as tobacco, alcohol or drugs (Dyckmans, 2012). In the group of 14 to 16-year-olds 17% of girls exhibit a generally problematic Internet use as compared to 14% of boys Overall 100,000 dependent and 400,000 problematic users can be identified. Social networks are very important for females, whereas boys continue to focus more on games (Schröder, 2012).

Next to other problems, such as excessively easy payment systems (such as via the parental phone bill), the phenomenon of cybergrooming is largely unknown. Cybergrooming is the planning and approach phase that precedes and initiates a sexual assault on a minor by an individual (Rüdiger, 2012). The anonymity and the lack of privacy settings provide paedophiles with easy access to potential victims. This problem can be applied equally to online games and their security setting, especially as online games are used increasingly frequently on social networks. Situations involving many children and uncontrolled communication will also attract offenders. According to the current KIM study, today a quarter of all children have already been sexually harassed on the Internet. A US study shows that 48% of the victims of Internet-based sexual offences were between 13 and 14 years old. Actual abuse is increasingly starting in the virtual world: 10% of rapes are initiated on the Internet (Finkelhor, 2008).

Girls are more commonly affected than boys. Only 8% can speak to their parents or friends about it (Katzer, 2007). Children are often at a loss as to what to do. Many parents are unaware of this problem and the public discourse tends to centre solely around the issue of data protection on social networks. Cybergrooming is often trivialised, although presenting a child with written materials or pornographic images to induce them to engage in sexual activity is actually an offence under section 176 (4) (3) and (4) StGB.

This is primarily a generational problem given that most parents grew up with letters, postcards, fax machines and early computers such as the VC 64 in Germany. Access to the World Wide Web affords previously unimagined opportunities of global communication that did not exist in the age of letters and postcards. This enables people to meet and/or stay in touch with others easily. Research and locating information has also been vastly simplified. The immediacy offered by the Internet would otherwise be almost impossible. Although this article deals with the risks and dangers of the Internet for children and young people, it is worth not losing sight of the opportunities afforded by the Internet.

However, in order to be able to use these advantages safely, more politicians and service providers need to accept greater responsibility. These should ensure that effective protective mechanisms are in place and that comprehensive, systematic and targeted media competence training is established not only for children and young people, but also their parents and teachers in order to close the generational gap.

3. Competences in the online protection of minors in Germany: Who? What? When?

One of the basic problems for the protection of minors on the Internet in Germany is that in the past attempts were made to transfer existing mechanisms for the protection of minors from the real to the digital world – an approach that is doomed to fail. A printed publication can be confiscated, pulped and its distribution prohibited. This is not possible for online media due to the limitless distribution opportunities and the associated collective memory. The Internet never forgets. In this context the debate about blocking pages depicting child pornography, that is, images of abuse, is worth mentioning. Both child protection organisations and politicians initially believed that this problem could be tackled by means of a technical block. It only became clear that this was neither technically feasible – blocks can quickly be circumvented – nor reasonable in terms of the basic understanding of the Internet – there is a risk of such images being transferred to other pages or even to private networks – after an intensive and occasionally very emotional debate.

Access to the World Wide Web affords previously unimagined opportunities of global communication that did not exist in the age of letters and postcards.

Given that on the one hand state monitoring of the Internet is neither possible nor wanted by any party, and on the other self-regulation of the markets is not producing the desired success, in Germany trust is being placed in the principle of regulated self-regulation. This management concept is defined as self-regulation that takes place within a legal framework that the state has imposed in order for the regulatory objectives to be achieved (Schulz, Held, 2002).

So what can be done to establish an effective system of protection of minors nonetheless? In order to examine this question, the legal framework will be discussed here. Which law is relevant for the protection of children and young people on the Internet? The legal framework and points of contact are not uniformly governed in Germany because there is not just one law and one point of contact.

In order to introduce child protection in the media in Germany, three relevant statutory bases will be presented and described. Worthy of particular mention are the German Protection of Young Persons Act (*Jugendschutzgesetz,* JuSchG), the Interstate Treaty on Child Protection in the Media (*Jugendmedienschutz-Staatsvertrag*, JMStV) and the German Criminal Code (*Strafgesetzbuch*, StGB). As well as the relevant institutions and processes, existing deficits will be discussed.

3.1 Protection of Young Persons Act

These, usually free (with the exception of very costly virtual goods that can be purchased) games on the Internet are in truth accessible to anyone and are not subjected to any examination procedure.

At the national level the Protection of Young Persons Act has been protecting children and young people in public and in the area of media since 1952. Since 2003 this Act has also governed the age certifications for computer and video games. Like films before them, games are tested and their content evaluated and correspondingly only approved for certain age groups. In 1994 the Entertainment Software Self-Regulation Body (*Unterhaltungssoftware Selbstkontrolle*, USK) was set up under the Protection of Young Persons Act as the responsible body for the age rating of video games. Under section 14 JuSchG the Supreme Regional Youth Protection Authorities (*Oberste Landesjugendbehörden*) are responsible for age rating. In collaboration with the representatives of the German federal states (*Länder*) at the USK, these have the ultimate decision-making authority as regards age rating. This approval is definitive for retailers: games must be clearly labelled and may only be sold to the age group to which the approval applies. However, it has to be said that JuSchG does not cover all types of game, only those that are sold on storage media. This does not include purely server-based online games as these cannot be bought in shops. These, usually free (with the exception of very costly virtual goods that can be purchased) games on the Internet are in truth accessible to anyone and are not subjected to any examination procedure. This key aspect of the online world is therefore not legally regulated by the JuSchG.

Sections 17 to 25 JuSchG provide for a further actor for the examination of compliance with the stipulations under the JuSchG: the Federal Review Board for Publications Harmful to Young Persons (*Bundesprüfstelle für jugendgefährdende Medien*). This Supreme Federal Authority, subordinate to the Federal Ministry of Family Affairs, Senior Citizens, Women and Youth (*Bundesministerium für Familie, Senioren, Frauen und Jugend*), can include written material and audio and visual media in the list of titles harmful to minors (indexing) and thus substantially restrict distribution. Indexed games may not be traded freely (section 15 JuSchG). The associated sales ban has a huge negative impact and is circumvented by many games producers by creating abridged versions and versions edited for the German market. In Germany computer games sold on physical media have to be tested by the USK to prevent them from being classified as harmful to minors and indexed from the outset (section 12 (5) JuSchG).

The basic idea behind age rating is to create a standard and binding identification signal for parents and consumers to offer certainty when purchasing games.

3.2 Interstate Treaty on Child Protection in the Media

Although the USK now offers testing procedures for age rating both computer and video games on physical media and computer and video games on the Internet and other telemedia content, the testing procedure of telemedia content and services takes place without state involvement – so it is not a mandatory requirement and there are no consequences for non-compliance. Such content falls within the scope of the Interstate Treaty on

Child Protection in the Media (JMStV) agreed between the German federal states. Since 2003 the JMStV has covered not only radio and television, but also content and services as well as online games offered on the Internet. Yet, this does not neatly close the lacuna arising under the JuSchG as is shown below. Pursuant to sections 14 et seq. JMStV, the Commission for Child Protection in the Media (*Kommission für Jugendmedien-schutz*, KJM) monitors compliance with the provisions of the Interstate Treaty on Child Protection in the Media. The KJM is supported by various companies (e.g. Jugenschutz.net under section 18 JMStV) and other institutions of voluntary self-regulation recognised by KJM pursuant to section 19 JMStV (FSK, FSF, FSM, USK). The latter, deployed as child protection officers, satisfy the obligation arising under section 7 JMStV for "commercial providers of generally-accessible online offerings that include content relevant to the protection of minors" (section 7 (1) JMStV).

As regards telemedia content (excluding current political events if there is a justified interest in this specific form of presentation or reporting (section 5 (6) JMStV)), several options are set out to adequately ensure that children and young people do not come into contact with inappropriate content (section 5 (3), (4), (5) in combination with section 11(1) JMStV):

- Restriction of access times
- Use of technical or other means to restrict access
- Programming for one of the child protection programs accepted by the JVM

Section 5 (4) JMStV offers the opportunity to provide access to content not approved for minors exclusively between 11:00 p.m. and 6:00 a.m. and content for the over 16s only between 10:00 p.m. and 6:00 a.m. Further access restriction can be achieved by using an age-verification positively evaluated by the KJM. Access protection should be ensured by two steps: "firstly by means of at least one one-off reliable check that the individual is of age (identification) that must take place by way of personal contact; secondly by way of secure authentication on every use to minimise the risk of multiplication, passing on or other abuse of access data to minors." (Döring, Günter, 2004, p. 232). The system will not be considered effective if the age is verified via the ID card number as such numbers are easy to falsify or obtain via the Internet. Nonetheless, the technical measure to be taken must be proportionate in any event and may not infringe constitutional principles. In general KJM recommends the use of a Postident procedure.

Because providers rarely want to restrict their access – be that temporally or by a closed group – many will take the route of programming with an age rating pursuant to section 5 (3) no. 1 JMStV in combination with section 11 (1) JMStV. This sounds more complex than it actually is and is explained for example on the USK website (USK, 2012). In technical terms an age label which can be read by child-protection software is stored in the website's main directory. If parents have set these programs up accordingly, they prevent access to a page that has a higher age rating than approved for the user.

Similarly, content is not per se suitable or unsuitable for children and young people. For that reason individual gradations should be made depending on age.

The Internet cannot be cleansed and the option of general filters is neither desirable nor technically feasible. Similarly, content is not per se suitable or unsuitable for children and young people. For that reason individual gradations should be made depending on age. In light of that, the use of child-protection software pursuant to the Protection of Young Persons Act and the Interstate Treaty on Child Protection in the Media the only reasonable alternative. As already shown at the beginning, however, too few parents use corresponding child-protection software to adequately protect their children. By way of reminder: only around a fifth of parents have installed such a program (Hasebrink, 2011). It is doubtful whether all 20% use a program for identifying the age label recognised by KJM. Further, the correct settings need to be made in these programs to prevent children and young people accessing unlabelled pages Unfortunately parents can only install such programs on their own computers; they have no control over what goes on outside their own home.

Since 2011 the USK has also been recognised for the age rating of, and appointed as the child protection officer for, online games pursuant to section 19 JMStV. However, this law does not impose a testing obligation. The provider alone decides which age group the content and services are suited to. The providers of server-based online games can access a free label generator provided by the USK that can be used to display an age rating. However, in technical terms this label is only visible to child-protection programs. Parents who want to find out about the game on the web page do not see this label. If the game can also be bought on data-storage media, the provider merely needs to visibly display the USK mark that is found on the packaging of the game either in text form or as a symbol on the web page under section 12 JuSchG and JMStV. Further, on 8 February 2012 the child-protection programs of Deutsche Telekom, member of the FSM, and JusProg e.V. were first recognised by the Commission for Child Protection in the Media (KJM, 2012).

It should be remembered that there is a legal lacuna in relation to purely server-based online games: an age rating is not displayed to the user on the page, but can only be recognised by upstream child-protection software.

3.3 German Criminal Code

A further legal basis relevant to the issue of cybergrooming is the German Criminal Code (*Strafgesetzbuch*, StGB). However, the StGB again does not provide adequate protection against the spread of cybergrooming on the net as preventative measures cannot be taken against cybergrooming. Specifically the law says:

> *"Whosoever […] presents a child with pornographic illustrations or images, audio recording media with pornographic content or pornographic speech, [...] shall be liable to imprisonment from three months to five years." (section 176 (4) StGB)*

Subsection 6 continues:

> *"The attempt shall be punishable; this shall not apply to offences under subsection (4) Nos 3 and 4 and subsection (5) above." (section 176 (6) StGB).*

Thus, the attempt alone is not punishable. Spectacular cases such as "Operation Donau" by the Tuttlingen police showed that the legal position is not sufficient to put an effective stop to cybergroomers' activities before a further offence such as the possession of child pornography or actual abuse is committed. The section of the StGB is fundamentally not geared to the situation on the Internet: in a playground there would be no need to ask the question whether there was an attempt to present a child with written materials to induce them to engage in sexual activity or whether it actually happened. To prevent criminal offences, no police officer will act as a child and wait to be spoken to. On the Internet a different situation presents itself: in order to prosecute crimes, it would therefore be necessary to work with children as bait. In legal terms police officers and detectives disguised as children have no basis to intervene, even if the opposite party assumes that a child under 14 is on the other side of the screen. The law enforcement agencies can only act if there are for example indications of the possession of pornographic material depicting children. Although cybergrooming is defined as the approach phase for the sexual abuse of children (Rüdiger, 2012) and often leads to actual abuse (Finkelhor, 2008), the custodians of the law merely

To prevent criminal offences, no police officer will act as a child and wait to be spoken to. On the Internet a different situation presents itself: in order to prosecute crimes, it would therefore be necessary to work with children as bait.

have a monitoring function as the law stands. However, this should not be dismissed out of hand. If there is no monitoring, offenders are not interrupted and can act unimpeded. This makes educating the population all the more important: incidents involving children need to be reported in order to be properly investigated.

4. Age rating of games and telemedia content

An important instrument in the protection of children and young people is the age rating of content – be that by way of a printed label on the packaging that attracts parents' attention – or in pure technical terms as a label that can be read by child-protection software. Here the individual topics will be mentioned only briefly without going into any detail on the harmful impact on development. Further, the problems of current labelling will be explained. As neither the Protection of Young Persons Act nor the Interstate Treaty on Child Protection in the Media contains a precise definition of the concept of harmful impact on development, the explanation of the definition pursuant to FSM, one of the recognised institutions of Voluntary Self-Regulation (*Freiwillige Selbstkontrolle*, FSK) pursuant to section 19 JMStV, shall be used. Similarly, the stipulations of the USK are applied.

4.1 Harmful impact on development pursuant to JMStV and Protection of Young Persons Act

The concept of harmful impact on development arose during the amendment of the JMStV in 2003. However, it was not precisely defined at that point.

The Interstate Treaty on Child Protection is worded as follows:

> *"Where providers distribute or make available offerings that are capable of impairing the development of children or young people into autonomous and socially-competent personalities, it is their responsibility to ensure that children or young persons of the age group in question do not usually come into contact with such offerings." (section 5 (1) JMStV)*

The FSM arrived at a definition in the first decision of its board of complaint:

> *"Offerings that, by significantly disrupting the standard sphere of experience of children and/or young people, may have a negative influence on the development of the personality of children and young people that contradicts the view of human beings set down in the German Basic Law (Grundgesetz) and thus interrupts or sets back their development into an autonomous person capable of freely developing within the social community." (FSM, 2004)*

This frequently-cited definition contains the question of the effects on acts, attitudes and spheres of experience of children and young people. The measures of worth derived from the German Basic Law are seen as determinative in our society. The following deserve particular mention in the context of classifying the content into the categories of erotica, violence and extremism:

- Respect for human dignity
- Equality
- Democratic principles

Further, the classification of harmful impact can be determined by age groups as children and young people of different ages are also differently susceptible to harmful impact on development. There are therefore no generally applicable yardsticks for children and young people; instead these need to be seen in context (FSM, 2004).

The USK Advisory Council determines and adapts the evaluation criteria of the USK. The concept of harmful impact on development is defined as follows in the USK principles:

> *"Harmful impact is defined to be*

n important instrument in the protection of children and young people is the age rating of content – be that by way of a printed label on the packaging that attracts parents' attention – or in pure technical terms as a label that can be read by child-protection software.

> *inhibitions, behavioural disturbances or damage caused by overstimulation, excessive stress or over excitation. In particular the content of games "which inhibit character, moral (including religious) and mental development, which cause disturbance or damage or which exert a disorienting effect in social ethics terms [may impair] the development of children and young people or their progress to becoming an autonomous and integrated member of society." (section19 (2) USK Principles)*

The USK examines 15 different dimensions of games that are considered to have an influential impact (USK, 2011):

- Audiovisual realization of the game concept
- Gameplay
- Atmosphere
- Realism
- Authenticity
- Human likeness
- Appeal to young people and identification potential
- Pressure to act
- Violence
- War
- Fear and threat
- Sexuality
- Discrimination
- Language
- Drugs

The USK's explanations of its principles show that the sole consideration is the static content of games and telemedia content and their impact. However, only the abovementioned aspects are deemed to have a relevant effect.

The USK gives weight to a great many dimensions; however, this perspective includes nowhere the risk of a child becoming the victim of an offence. The fact that children are also exposed to other dangers that lie outside the USK criteria is completely ignored. For example, not only server-based games, but also console games offer the opportunity to make contact that can lead to sexual harassment. This concept of victimisation is not included in the considerations for the classification of games, online services and content.

Whilst games on physical media are tested by the USK, the JMStV calls on providers of online games and other telemedia content and services to themselves assess the extent to which the content and services offered may have a negative impact on development. The basic requirement for this is the ability to put oneself in the mindset of young people, to appreciate the influential impact of the medium of the Internet within the everyday lives of the age groups in question and to know the constitutionally-relevant values of our society.

4.2 Age rating and cybergrooming

The USK or FSM criteria are by no means set in stone. They could be adapted and extended. This is to be welcomed in relation to the problem of cyberbullying, and more so for cybergrooming, because an important point has so far been ignored and the criteria need to be supplemented in order to offer effective protection against victimisation: the risk of anonymous online communication.

This is to be welcomed in relation to the problem of cyberbullying, and more so for cybergrooming, because an important point has so far been ignored and the criteria need to be supplemented in order to offer effective protection against victimisation: the risk of anonymous online communication.

Age ratings do not deal in any way with the risks of cybergrooming. The classification criteria discussed above for online media and games are unsuitable for identifying potential risks, let alone tackling them. All previous classification criteria are primarily based on examining the content of the game for the potential to impair or jeopardise development. In essence all that age classification deals with is whether the game contains excessive and/or inhuman levels of violence and/or whether pornographic content is presented. The criteria used for age classification are still based on the assumption that the user plays alone and not communicating via the Internet. However, this is no longer in line with how media are used today. Nowadays hardly any games can conceive of not offering an option for online-based interaction. The interaction and communication processes that take place carry the risk of serious offences being committed between the users. The anonymity of the Internet encourages the particularly serious phenomenon of cybergrooming, which is extremely dangerous for children. The graphic design of a whole raft of online games and social platforms is targeted at children and young people (cf. Habbo Hotel, NeoPets, Knuddels). It is therefore natural that such unsecure games and services used by children are also extremely attractive to paedophiles. Providers should be obliged to integrate protective mechanisms as far as possible that prevent these risks of cybergrooming to the same extent as it targets or accepts children. However, almost all games today lack effective security precautions – irrespective of whether they are available as physical media or purely online.

Providers should be obliged to integrate protective mechanisms as far as possible that prevent these risks of cybergrooming to the same extent as it targets or accepts children.

It is important to note that many children and young people do not even realise that they have been the victim of a criminal offence and this issue of sexual advances and harassment is trivialised within society. Many parents are neither aware of this phenomenon, nor do they realise its extent. This can first be explained due to a generational conflict which produces a situation where parents, teachers and other persons of trust are unable to act as competent points of contact. Most parents do not look at the pages their children visit on the Internet and therefore are not aware of the specific dangers posed there. Second, even parents who take the protection of children and young people seriously rely on the official age ratings of the USK and the other competent actors. This where action is needed and the criteria for the age ratings revised.

Unregulated voluntary action and existing measures such as the appointment of a youth protection officer pursuant to section 7 JMStV, who has no authority whatsoever to issue instructions for dealing with cybergroomers, or a pure block or ignore function are quite simply not enough. This in no way renders the offenders ineffectual. They would simply aim their approaches at the next child, or use a new account to approach the same child again (Rüdiger, 2012).

5. Need for reform

Given that the phenomenon is not limited to Germany, partnerships need to be developed that where possible also take particular account of cultural differences, even if it is not realistic for an international strategy to be realised in the short term. Conflicts even within Germany surrounding the issue of child protection in the media show that we are still a long way away from an international solution. For that reason reform proposals for Germany at least will be presented here.

5.1 Legal reform of child protection in the media

Given the fluid boundaries between online and offline, including with computer games, we see how essential a single point of contact and statutory basis is that comprehensively covers the topic of child protection. A differentiation between computer games on physical media and server-based ones that imposes differing obligations as regards the protection of children and young people does not reflect reality and is quite frankly antiquated. Alongside standardisation, the dynamics of the processes need to be taken into account. Complex statutory amendments that invariably unleash an ideological battle cannot offer any level of effective child protection in the media that reacts to changes in the market. For that reason regulated self-regulation should be seen as the way forward.
Unlike conventional media, the nature of the Internet affords opportunities for

interaction. The anonymity on the Internet lowers the inhibitions that could protect children and young people from victimisation in the real world, e.g. in the playground. In order to effectively pursue cybergroomers, the Criminal Code needs to be revised to make the very attempt an offence. The focus should be on the intention of the offenders.

In view of the fact that the law differentiates between children, young people and adults, age groups should be adapted accordingly to prevent there being too many age groups on the Internet. A key contribution here are age verification systems in the form of closed groups as set out in section 5 JMStV. This form of access restriction, chosen by the provider itself, should be promoted more vigorously. Incentives should be created to make it difficult for children to access harmful content, even if they specifically seek it out. Conversely, more and above all secure surfing space needs to be created for children and young people.

Specifically, conditions may be imposed that oblige providers to offer better protection for children and young people if they specifically aim their games at children: unsupervised communication channels put children and young people at risk of becoming a victim of cybergrooming or other crimes.

5.2 Paradigm shift regarding "harmful impact on development"

It is not only the statutory position that needs to be simplified, but the transparency regarding the issue of age ratings also requires improvement. Only after precise research can content and services be classified. However, how are consumers, parents and children to know what the age classification entails when they pick up a product in their hands in the shop? Printing the familiar label of the USK even larger on the packaging is of little use. Instead, what it actually signifies should be made clearer. One option would be to work with small symbols, such as the pan-European PEGI system, that provide more accurate information about what can be expected from this game or content.

What is also important is that the standard statutory assumption of the sole player is abandoned and the risks of anonymous and generally uncontrolled online communication are heeded and included in the assessment. The foregoing discussion regarding USK's criteria for issuing age ratings produces the following recommendations for improvements regarding the classification of harmful content and services for children and young people.

In the first instance there is a need to adopt a fundamental criterion for securing the communication channel for online games within the principles for evaluating games and content. The new criteria should apply not only to purely server-based online games, but also console games (Wii, X-Box, Playstation, Nintendo DS etc.), as these also offer the opportunity for online communication.

Specifically, conditions may be imposed that oblige providers to offer better protection for children and young people if they specifically aim their games at children: unsupervised communication channels put children and young people at risk of becoming a victim of cybergrooming or other crimes. One solution is communication exclusively by means of pre-defined sentences and words, as is already operated by certain child-appropriate chats. Also, the permanent presence of qualified moderators can be an effective protective measure. Children should not be able to take part in unsupervised chats. The quality of the moderators, i.e. supervisory personnel and contact persons of a game or chat, should be ensured. They are often the first point of contact for children following sexual victimisation. At present operators primarily deploy untrained lay personnel, known as game masters, who are recruited from the gaming fraternity. A youth protection officer appointed under the Interstate Treaty on Child Protection in the Media cannot assume this role alone as this is inadequately specified under the JMStV, nor does it have any influence over the quality of the other moderators. An obligation to undergo associated training or proof of certification would be an important step in order to deal expertly with the consequences of sexual or other victimisation. Certification similar to a certificate from the Chamber of Trade and Industry could be set up. To prevent people with criminal motives being used as moderators, the presentation of an extended police record of good conduct should be mandatory.

As already outlined in the previous section, the discrepancy between the law and classification criteria needs to be reconsidered. The age categories for games, telemedia content and services should be simplified – not only because it is difficult for many providers to classify their own content correctly. Further, the law makes a distinction between children, young people and adults. In the eyes of the law you are a child until the age of 14, and a young person from 14 to 18. A classification, or at least a consideration, of this important age group is important for the protection of children and young people. The scope of protection from sexual abuse and cybergrooming under section176 (4) (3) StGB covers people under 14, i.e. to children. This necessarily results in a discrepancy in terms of the current age groups of the labels “approved for 12 and over” or “16 and over”. On the one hand the law penalises sexual communication with children under 14, but on the other gives parents a false sense of security through the age approval from 12 years and above. This suggests that playing online games and the associated unsupervised communication is risk-free. For that reason the age limit of 14 years as provided for in the StGB should also be taken into account in the USK’s age rating.

5.3 Include media competence in the syllabus

In closing we shall look at a key component regarding child protection in the media that is also often ignored by the political sphere: the issue of media competence. The issue here is to familiarise young people with the digital world at as early an age as possible, as well as instilling competence in parents and teachers, who are often unaware of what the Internet means to children. Further, parents and teachers are also to an extent overwhelmed by the topic or are not interested in it. In many cases they lack fundamental knowledge about social networks, opportunities and mechanisms on the Internet as well as communication and interaction opportunities in online games and chat forums. The current training landscape, in particular the schools, has not yet arrived in the 21st century in this regard. Even if the issue of Internet security is a proposed subject on the syllabus of 23 countries across Europe, the subject is the preserve of committed teachers, individual initiatives on the ground or NGOs. This topic, which is crucial not only for the future of children, but also society itself, is not accorded the significance it deserves in syllabuses nor in teacher training.

General compulsory education has ensured that all children living in Germany have the opportunity to learn to read and write. This includes children of all classes and nationalities and is one of the guarantors of equality of opportunity and social justice. In the field of media competence it is primarily the children of parents who read newspapers who are reached by net and flyer campaigns, but not those who are already disadvantaged and whose media consumption is way below average. These issues require mandatory inclusion in teacher training. Media driving licenses should not be optional, but a fixed component of the syllabus. It is important that the standard lessons in kindergarten and school also access parents in order to integrate them, too. This cannot be made solely the school’s responsibility – without parents the protection of young people will not and cannot work as a general task of the education system. In order to embed comprehensive media competence in the syllabus, to include parents as well as to make teachers and educators net-savvy,

The issue here is to familiarise young people with the digital world at as early an age as possible, as well as instilling competence in parents and teachers, who are often unaware of what the Internet means to children. Further, parents and teachers are also to an extent overwhelmed by the topic or are not interested in it.

the government, providers, the public sphere and schools all need to be pulling in the same direction.

It also makes sense to embed these endeavours in the German Protection of Young Persons Act and the Interstate Treaty on Child Protection in the Media. This should deal not only with obligations, but also specific measures. The majority of NGOs already have the will, but insufficient means to enable them to make an optimum contribution to imparting media competence. Public-private partnerships could serve to combine the standardising and controlling qualities of the state with the commitment of NGOs as well as the financial means, technical resources and the excellent distribution opportunities afforded by providers.

Good practice should be established so that sensitisation campaigns reach all children, parents, teachers and carers across the EU at all times. Effective sensitisation strategies take into account the different states of development of younger and older children and young people and concentrate in particular on the youngest children and those most in need of protection, including those with learning difficulties and mental disabilities. At the same time mutual education amongst children of different ages represents an important strategy in making children of all age groups aware of their rights and responsibility in the online context.

In line with the concept of voluntary self-regulation, the resources of the Internet community and users should also be used. These are directly involved in actual events and could provide useful pointers. This means that self-regulation is not only ensured by providers, but also the users.

6. Conclusion and outlook

The need for reforming child protection in the media in Germany has been demonstrated.

The need for reforming child protection in the media in Germany has been demonstrated. The announcement of a planned reform of the German Protection of Young Persons Act on 13 April 2012 by the Federal Ministry of Family Affairs, Senior Citizens, Women and Youth to have online films and online games labelled in accordance with the provisions of the Protection of Young Persons Act is just a first step. What we need is a true paradigm shift. It is crucial that the distinction between the virtual and real world in people's minds is removed and a uniform, transparent law with one point of contact for the protection of children and young people is put in place. Few parents currently deploy child-protection programs. For that reason it also makes sense to point out to parents and consumers the importance of age labelling in the scope of child protection in the media. This mark should also be identifiable at first glance for online games. It is also important not only to evaluate the Internet's static content when it comes to the protection of young people. Rather, the communication channels – the dynamic processes – also need to be part of the consideration of the context to tackle the potential victimisation of children and young people.

This needs to take into account the fact that the development of technologies is advancing at an ever-increasing pace, meaning that there is usually little time for time-consuming amendments to the law. Germany's inability to react dynamically to changes in the market can be seen by the fact that the treatment of online games is still not adequately regulated in Germany, whilst for instance the pan-European system PEGI – which applies in all other European countries – has covered online games since 2003 and included apps for smartphones and tablets in its evaluations as early as 2012.

A further issue poses an even greater problem than the speed of market development for the protection of children and young people: as early as 2008 Google announced that there are now 1 trillion URLs on the Internet (Google, 2008). This figure has in all likelihood increased since then. Conversely there are currently over 15 million pages with a ".de" domain (DENIC eG, 2013). Although this is not the equivalent of all pages originating in Germany, it can be assumed that the German legal position can only regulate a fraction of pages that can be accessed in Germany through the Protection of Young Persons Act, the Interstate Treaty on Child Protection in the Media and the German Criminal Code. These laws have no influence over pages that lie outside the jurisdiction that ends at the borders of the Federal Republic of Germany. In the long term only cross-border cooperation can result in effective protection against content that is capable of having a negative impact on society.

In order to provide children and young people with an adequate level of competence, to make them secure in their values and to sensitise society accordingly, the issue of media competence should be embedded in school syllabuses. IT is already offered as a working group or a taught subject in many secondary schools. However, the focus there is more on technical aspects and less on social competence on the Internet.

It is essential for preconceptions and entrenched positions to be overcome if standardised protection of children and young people is to be established. Net activists should be increasingly integrated into child protection in the media to prevent them from being forced into an oppositional corner. Free expression of opinions and access to information are not contrary to the protection of children and young people. Good solutions require competent specialists who devise and test recommendations to make the Internet safer for those who urgently require society's protection: children and young people.

7. Literature

Google (25 July 2008): We knew the web was big… Alpert, Jesse; Hajaj, Nissan. Available online at http://googleblog.blogspot.de/2008/07/we-knew-web-was-big.html, last checked on 14 January 2013.

DENIC eG (14 January 2013): www.denic.de. DENIC eG. Available online at www.denic.de, last checked on 14 January 2013.

Döring, Martin; Günter, Thomas: Jugendmedienschutz: Alterskontrollierte geschlossene Benutzergruppen im Internet gem. § 4 Abs. 2 Satz 2 JMStV. In: MMR, 4/2004, pp. 231-237. Available online at http://www.jugendschutz.net/pdf/mmr_avs.pdf, last checked on 14 January 2013.

Dyckmans, Mechthild (2012): Drogen- und Suchtbericht. Ed. by Die Drogenbeauftragte der Bundesregierung. Available online at http://www.drogenbeauftragte.de/fileadmin/dateien-dba/Presse/Downloads/12-05-22_DrogensuchtBericht_2012.pdf, last checked on 14 January 2013.

Finkelhor, David (2008): Childhood victimization. Violence, crime and abuse in the lives of young people. New York: Oxford University Press.

Freiwillige Selbstkontrolle der Multimedia-Diensteanbieter (2004): Der Begriff der Entwicklungsbeeinträchtigung in § 5 des Jugendmedienschutz-Staatsvertrags. Ed. by FSM. Available online at http://www.fsm.de/de/entwicklungsbeeintraechtigung, last checked on 14 January 2013.

Haddon, Leslie; Livingstone, Sonia; EU Kids Online network (2011): EU Kids Online: National perspectives. Ed. by EU Kids Online. Bristol. Available online at http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/PerspectivesReport.pdf, last checked on 14 January 2013.

Hasebrink, Uwe; Lampert, Claudia; Schröder, Hermann-Dieter; Drosselmeier, Marius (2011): Jugendmedienschutz aus

Good solutions require competent specialists who devise and test recommendations to make the Internet safer for those who urgently require society's protection: children and young people.

Sicht der Eltern. Kurzbericht über eine Studie des Zweiten Deutschen Fernsehens. Ed. by Uwe Hasebrink. Hans-Bredow-Institut für Medienforschung an der Universität Hamburg. Hamburg. Available online at http://www.unternehmen.zdf.de/fileadmin/files/Download_Dokumente/DD_Das_ZDF/Veranstaltungsdokumente/ZDF-Studie_Jugendmedienschutz_aus_Sicht_der_Eltern_2011.pdf, last checked on 14 January 2013.

Katzer, Catarina (2007): Gefahr aus dem Netz. Der Internet-Chatroom als neuer Tatort für Bullying und sexuelle Viktimisierung von Kindern und Jugendlichen. PhD thesis. Cologne University, Cologne. Faculty of Economics and Social Sciences, last checked on 14 January 2013.

Kommission für Jugendmedienschutz (9 February 2012): KJM erkennt erstmals zwei Jugendschutzprogramme unter Auflagen an. Kommission für Jugendmedienschutz Available online at http://www.kjm-online.de, last checked on 14 January 2013.

Medienpädagogischer Forschungsverbund Südwest (2011): KIM-Studie 2010. Kinder + Medien, Computer + Internet. Ed. by Medienpädagogischer Forschungsverbund Südwest. Stuttgart. Available online at http://www.mpfs.de/fileadmin/KIM-pdf10/KIM2010.pdf, last checked on 14 January 2013.

National survey of American attitudes on substance abuse XVI: teens and parents (2011). Conducted by: QEV Analytics, Ltd. Knowlegde Networks. The national center on addiction and substance abuse at Columbia University.

Rüdiger, Thomas Gabriel: Cybergrooming in virtuellen Welten – Chancen für Sexualstraftäter?, 2/2012). In: Deutsche Polizei, 2/2012, pp. 29–35. Available online at http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&ved=0CEwQFjAD&url=http%3A%2F%2Finstitut-kreative-wissenschaft.com%2Fapp%2Fdownload%2F5780972045%2FCybergrooming%2Bin%2Bvirtuellen%2BWelten%2BDeutsche%2BPolizei%2B2_2012.pdf&ei=Nmf0UImhA8ntsgbe44GACg&usg=AFQjCNFzQRMGqjYN4qY6hdA23_6iE8w1Rw&sig2=FLUS4IaQoqgeO1KTi1QC9w&bvm=bv.1357700187,d.Yms, last checked on 14 January 2013.

LBS-Kinderbarometer (29 October 2012): Kinder und Internet: Kontakte pflegen ja – neue Freunde eher nicht. Dr. Christian Schröder. Available online at http://www.lbs.de/bremen/presse/initiativen/kinderbarometer/kinder-und-internet, last checked on 14 January 2013.

Schulz, Wolfgang; Held Torsten (2002): Regulierte Selbstregulierung als Form modernen Regierens. eine Studie im Auftrag des Bundesbeauftragten für Kultur und Medien (Endbericht). Ed. By Hans-Bredow-Institut für Medienforschung an der Universität Hamburg. Hans-Bredow-Institut für Medienforschung an der Universität Hamburg. Hamburg (Arbeitspapiere des Hans-Bredow-Instituts Nr. 10, 10).

Spitzer, Manfred (2012): Digitale Demenz. Wie wir uns und unsere Kinder um den Verstand bringen. Munich: Droemer Knaur.

Unterhaltungssoftware Selbstkontrolle (2011): Grundsätze der Unterhaltungssoftware Selbstkontrolle (USK). Ed. by USK. Available online at http://www.usk.de/fileadmin/documents/Publisher_Bereich/USK_Grundsaetze_2011.pdf, last checked on 14 January 2013.

Unterhaltungssoftware Selbstkontrolle (2011): Leitkriterien der USK für die jugendschutzrechtliche Bewertung von Computer- und Videospielen. Ed. by USK. Available online at http://www.usk.de/fileadmin/documents/2011-06-27_Leitkriterien_USK.pdf, last checked on 14 January 2013.

About the author

Ines Kawgan-Kagan was born in Berlin in 1982 and studied public administration at the University of Applied Sciences for Administration and Legal Studies and the sociology in the European Societies master's programme at the Free University Berlin. She is the mother of four children and up to December 2012 she dealt with issues including the protection of young people in the media at the Deutsche Kinderhilfe.

Technical approaches for the detection of criminal activities in online environments

Prof. Dr.-Ing. habil. Ulrike Lucke

Abstract

This article is focused on the discussion on Cyber-Grooming from a technical perspective. After a short introduction to the phenomenon and its societal significance, relevant online environments are presented. Moreover, the activities to be recognized in such worlds are discussed in more detail, and targeted approaches for their detection are presented. In the following, a methodology to automatically detect suspicious activities – based on current mechanisms from computer science – is proposed. The article concludes with a summary of possible countermeasures for Cyber-Grooming, including the prerequisites, outcomes, and limitations of technical detection mechanisms.

1. Which problem do we address?

The EU has explicitly admitted to making the Internet a safer place for kids and minors [8]. From a technical point of view, the discussion in the EU on protecting children is finally focused on the question to just block or completely delete harmful websites. This is not targeted to current online environments (like virtual worlds, browser games, or online apps), but is stuck to an out-dated content-oriented (not: communication-oriented) view on classic Web pages with text, images, audio, or video.

Moreover, those static Web pages are not in the primary focus of minor users. Kids primarily explore the internet by starting to play games, not by surfing the Web [16]. Those online environments are especially attractive because of their possibilities to interact and communicate with other players (like shared game experience, chats, etc. to find and maintain friendship). There are certain offers in the Internet with a design and game mechanism that is particularly suitable for children, where they are especially exposed to enter close emotional relationships with others. Besides other legal issues, this is intensively exploited by pedo-criminals in a targeted manner [3]. Such initiations of sexual interactions with minors are called Cyber-Grooming [5][15].

Kids primarily explore the internet by starting to play games, not by surfing the Web.

This important, but not yet sufficiently covered topic was primarily addressed by the symposium "Protection of Children and Minors in the Internet – Perils of Virtual Worlds" on 19 September 2012 in Brussels [9]. Starting from a criminological overview of the phenomenon, aspects of law, society and IT for protecting kids and minors against Cyber-Grooming have been considered by respective experts, and first experiences with virtual police offices in an online game for kids have been presented. In the following, the political consequences have been discussed with representatives of EU commission and parliament. All participants agreed that the Internet is an important part of today's media reality, and that providing related skills as well as an adequate protection of minors are a central goal of our efforts.

As a result, there were identified shortcomings of law, investigation, prosecution, and prevention; and a first catalog of possible countermeasures was gathered. Among others, a new age rating

Moreover, the development of technical means to detect and block suspicious activities in online environments were discussed, which need to be balanced between safety and privacy.

(age levels, criteria, and responsibilities), an adequate media-related instruction of kids as well as training of other involved players (teachers, police men, state attorneys, system providers), and a general sensitizing of the society for the perils of interaction and communication in the Internet were proposed. Moreover, the development of technical means to detect and block suspicious activities in online environments were discussed, which need to be balanced between safety and privacy. Further efforts to elaborate and implement the mechanisms mentioned above will follow in the near future.

This article presents a more detailed view on technical issues of how to detect and prevent criminal activities like Cyber-Grooming. In section 2, a short overview on covered systems is provided. Section 3 gives an impression of activities in those environments that can be automatically monitored. Section 4 presents some current mechanisms that can be facilitated to implement this, as well as an overall system architecture to realize detection and blocking of suspect activities. Finally, section 5 draws a conclusion of technical possibilities and necessary work.

2. Which platforms do we need to consider?

Public discussion on cases of Cyber-Grooming was mainly focused on specific platforms like Habbo Hotel[1] or Freggers[2]. They are explicitly designed for and offered to children. This comes along not only with special topics, stories, and designs, but also with simplified registration and authentication procedures that make it hard to lock out unwanted users.

In general, such online environments can be characterized as follows:

- Virtual worlds provide a more or less realistic copy of the real world, including places and typical activities to be carried out. Prominent examples are Second Life[3] (mainly targeted to adults), Habbo Hotel[1] (targeted to kids aged 12 to 18) or Panfu[4] (no age classification). They are accessed via browser interfaces or dedicated client software; the world models and interactions are buried on a central server. Virtual worlds do not offer a dedicated story or goal to their users, but are focused on the imitation of real-life activities and relationships. Users are present by means of their avatars, which are often far more different to their real-world counterpart than the world itself is. This opens up several possibilities for social interactions beyond traditional borders of ethnics, religion, age, or gender. This is of certain benefit for inclusion in settings like online learning [6], but can also be exploited by pedo-criminals to establish illegal contact with minors [5].
- Online games are associated with a specific story line, often based on a complex background philosophy, which requires the user to fulfill certain tasks or quests in order to reach a higher goal or level. Prominent examples are World of Warcraft[5] (scope: adventure, targeted to adults) or Oloko[6] (scope: farming, targeted to kids aged 6 to 12). Online games can also be played in the browser window or using dedicated client software; as in virtual worlds, the modeling and simulation of objects, avatars and interactions is realized on a central server. Because of the fictitious nature of a game, avatars are usually designed with lots of fantasy, hiding the real-life person behind it. While gameplay itself is headed towards a

[1] http://www.habbo.com/

[2] http://www.freggers.com/

[3] https://secondlife.com/

[4] http://www.panfu.com/

[5] http://eu.blizzard.com/en-gb/games/wow/

[6] http://www.oloko.com/

pre-defined goal (and therefore activities are usually restricted to this storyline), some platforms offer mechanisms for free interaction between users following a shared game experience. Again, this can be used for establishing unwanted or illegal contact between players [15].

- Mobile apps are a category which can be seen as orthogonal to the previous ones. Today, several platforms are extended by a mobile component for access via smartphones or tablet PCs. This includes both, virtual world simulations as well as game-based approaches. Moreover, some apps do not require an internet connection. Thus, they are not vulnerable to mis-use of communication features. Prominent examples are Nighty Night[7] (scope: animal care, targeted to kids ages 1 to 4) or WordFeud[8] (scope: word puzzle, targeted to player aged 10 or higher). Mobile access simplifies connection to the online environment and strengthens the relationship between the users and his/her digital self. As in above categories, apps can include traditional forms of communication and content dissemination, like chats or forums.

Platforms as described above are attractive to large amounts of users, because they are apparently different to the real world and allow them to escape from their every-day routine or the problems of adolescence. Moreover, they offer some kind of persistency that allows them to create an authentic experience for a high degree of immersion.

From the providers' perspective, attracting users is crucial for financial success. However, there are different business models. Some products require payment to enter the system, either for getting the software (e.g. app download) or as a monthly fee. This hurdle is often avoided for solutions targeting kids, since payment can usually not be realized without knowledge of resp. support by parents. Other products are free to use, but players have to pay for advanced features like weapons, furniture, pets, or food. This payment model may expose kids to financial dependency from other players, e.g. when they got a virtual pet as a gift and don't have means to feed it [20].

Considering these types and characteristics of online environments, technical mechanisms for monitoring of suspicious activities are restricted to server-based approaches for two reasons. First, stand-alone tools[9] do not support communication with other users and thus are not prone to mis-use for Cyber-Grooming. Second, governmental surveillance should keep away from private property and data of citizens (including their computers and software) [19], while commercial providers may be subject to regulation (e.g. for certification as a child-safe environment) and thus may be forced to install monitoring tools [22].

This payment model may expose kids to financial dependency from other players, e.g. when they got a virtual pet as a gift and don't have means to feed it [20].

3. Which activities do we need to monitor?

This section provides a more detailed analysis of activities in online environments that should be subject of monitoring. The focus is on issues that allow for an automated detection. This implies that there may be other events or content elements that would not be rated as harmful by technical solutions, but should be from a more general perspective. That's why

[7] http://www.goodbeans.com/products/nighty-night

[8] http://wordfeud.com/

[9] Theoretically, there is the third category of peer-to-peer applications, which is unequally harder to monitor. Those applications do neither rely on a central server nor do they reside on an single client, but they rather evolve from redundant, bilateral connections between nodes (clients) in a network. This architecture is well known from file sharing applications. However, there was not yet a case reported on illegal contact with children using such an approach.

accompanying approaches like virtual police officers in online worlds should be followed, additionally [13]. Moreover, automated detection implies a risk to find a supposed hit where no criminal or dangerous behavior took place. For this reason, technology can always just help to detect, to supply evidence, and to quickly react in questionable situations. However, technology can never judge on people. Personal rights, ethics and privacy are above any rating supposed by technology [10], and should be carefully considered during the design of a reporting system.

3.1 Text

The approach of using games theory addresses the inherent problem of predator and prey: Every action on one side causes the other party to adjust its strategy.

The most easy-to-monitor category of content elements is written or spoken language. (Spoken language can be translated into written text on-the-fly by voice recognition techniques [1]. Such systems have proven their maturity e.g. in telephony, in current game consoles and smartphones, or for supporting people with disabilities. Thus, spoken text can be automatically analyzed using the same methods as for written text.) If provided in written form, text can be searched for pre-defined patterns or any other irregularities that are used to classify if it contains unwanted content.

In general, an algorithm to monitor text messages and to rate them according to given threats [21] looks as follows:

1. if necessary, speech / character recognition
2. detection of bad words (and circumscriptions)
3. calculation of proximity measures
4. classification of message

The accuracy of results is determined by two variables, which come into play in steps 2 and 3 of this algorithm. First, the list of bad (i.e. unwanted) words needs to be defined, manually. This includes circumscriptions of these words (e.g. using so called ASCII art or wildcards) used by creative senders, e.g. “s3x” or “s_x” for the word “sex” [20]. That’s why emphasis should be put on management of those lists of bad words, e.g. using community approaches (providers and/or users that mutually exchange new bad words). Second, the validity of used proximity measures has a strong impact on the accuracy (average ratio of false positives and false negatives compared to the whole amount of text) of an algorithm. Here, the combination of several independent characteristics can be used to increase the overall accuracy.

Available mechanisms for e-mail spam detection demonstrate that such mechanisms work well for specific areas of application. However, there is some ongoing research on this topic that might be of interest for the detection of Cyber-Grooming attempts, as well. The approach of using games theory addresses the inherent problem of predator and prey: Every action on one side causes the other party to adjust its strategy. This can be facilitated for innovative detection mechanisms to break-through this loop [4]. Another approach is to use ontologies in order to recognize semantics behind a text. This can help to detect if somebody is obviously not speaking about what’s the primary meaning of his words, i.e. if there is an inconsistency in his message [7].

There are some alternatives to automated text classification that should be considered. If all communication (e.g. chat) is moderated by a human supervisor, sending of each message requires approval. This is realized for common office hours in some games like Panfu. Another option is to allow only pre-defined text blocks for messages, which should work for limited scenarios like sending friendship requests and status updates. Both mechanisms can be combined, e.g. only pre-defined text blocks as long as chat is not moderated. However, these mechanisms make sense only in small user groups, and they require the provider to pay some additional effort.

3.2 Graphics

While textual content is comparatively easy to analyze, visual information is harder to classify. This includes static images as well as dynamic media objects like animations or videos. Again, the latter, more complex types can be reduced to single, static scenes (so called frames) for analysis. This may not be necessary for every single frame, since modern video encryption is typically based on a number of intermediate frames containing only partial information derived from previous or following frames [14]. Thus, for reasons of performance video analysis may be restricted to so called i-frames containing complete scenes (e.g. one per 0,5 seconds in MPEG-1 and -2 videos, one per 10 seconds in MPEG-4 videos) without loss of precision.

As for textual content, a general algorithm for analyzing visual content may look as follows:

1. comparison with rated content
2. calculation of similarity measures
3. classification of image
4. if necessary, repeat this for single frames

Again, the quality of results is determined by two aspects. First, the specificity of pre-defined images has a strong impact. A database of very typical images of un-wanted content is required. Second, calculation of similarities between these images and the current content object is crucial. Objects may vary in size, color, direction, perspective, etc. — that's why several possible operations for transforming visual content (like scale, rotate, skew, distort, dye, shade, etc.) have to be applied and combined in order to test if any similarity to previously rated content can be created. The accuracy of results increases with the amount of rated content to compare, and with the complexity of comparisons to be carried out. However, the available time for processing is limited by the given ratio of frames to analyze, so a trade-off is necessary. Currently, a lot of research on visual computing is done, so new and improved algorithms will be available in the future [18]. Anyway, porn blockers have proven that these mechanisms can already work quite well.

Besides analyzing the content represented by an image or video, more simple (yet effective) means can be applied to the names and locations of these objects. For example, the name of a file may in some cases give a hint on its content, and it is much easier to analyze using the approaches presented in the previous section. Moreover, sites that are known to deliver un-wanted content can be handled in a similar manner, like successfully exploited for email spam detection (so called black or grey lists of hosts under suspect). Images or videos may only be subject of enhanced visual analysis if they successfully passed these simple tests.

There are some alternatives to automated verification of visual media, as for textual content. First, upload or linking of graphics may require approval by a moderator. Second, users can be forced to use pre-defined image libraries that are restricted to “safe” content. Again, a combination of these approached is possible, e.g. beyond office hours the use of individual content may be prohibited.

While textual content is comparatively easy to analyze, visual information is harder to classify. This includes static images as well as dynamic media objects like animations or videos.

3.3 Complex activities

The most complex types of activities to be detected are those consisting of individually un-suspicious elements that unfold their risk potential only in its entirety. Unfortunately, this corresponds to the most dangerous type of Cyber-Groomers who's patiently establishing a personal relationship to his later victim [20]. Thus, stream-based detection mechanisms as described above cannot help here. Rather, data on all interactions between users has to be logged in order to have it available for later analysis — a very critical approach in terms of privacy.

Obviously, it is not feasible to continuously transmit data on all activities of all users in all virtual worlds to a central law enforcement agency, even if limitations of national law were resolved. Besides respecting private interactions between users, the pure amount of incurring data will forbid this approach. Several means may help to cope with these problems:

- Suspicious activities follow typical patterns. This may be to send similar messages to a number of other users in short time, to repeatedly send messages to the same person by using different accounts, or to unilaterally finance the virtual belongings of another user. Not all aspects of interactions need to be logged, but only the elements of those patterns.
- For detection of those patterns, it is not necessary to know the exact identities of related users, but just to differentiate between several accounts and user classifications like age-range and gender. Thus, identities of users can be hidden by assigning pseudonyms[10] which can be resolved only by the providers of virtual worlds. This can be compared to masking the origin of a computer by an IP address, which can be resolved by the responsible internet provider.
- Finally, information on users and their interaction should remain inside the platform of the provider as long as possible in order to avoid misuse. Accumulated reports can be transmitted to law enforcement agencies, which in turn can request to fully log data on relevant users and their interactions in order to collect evidence.

Thus, identities of users can be hidden by assigning pseudonyms which can be resolved only by the providers of virtual worlds.

However, this requires the discovery of typical activity patterns of Cyber-Groomers as well as their formal description.

Additionally, established community mechanisms like report-buttons for users can help to collect relevant information. Users can provide hints on suspicious behavior with just a few clicks. This creates valuable data for automated detection mechanisms, since preceding activities can act as training data, too.

3.4 Putting it all together

The combination of all methods described above leads to a multi-level approach for the detection of suspicious online activities. The following diagram provides a graphical representation of these mechanisms, using the notation of a process model. Logging all communications and item-based interactions, as well as analyzing communications are parallel processes, accompanied by optional human moderators and virtual policemen. Please note that the focus of the presented process model is on monitoring tasks, i.e. common activities of users or providers of online environments are displayed only as long as they are relevant for the detection of suspicious activities.

[10] Please note that users of online environments typically act under a user name, so later assignment of pseudonyms to these user names is yet a second step to hide their identity.

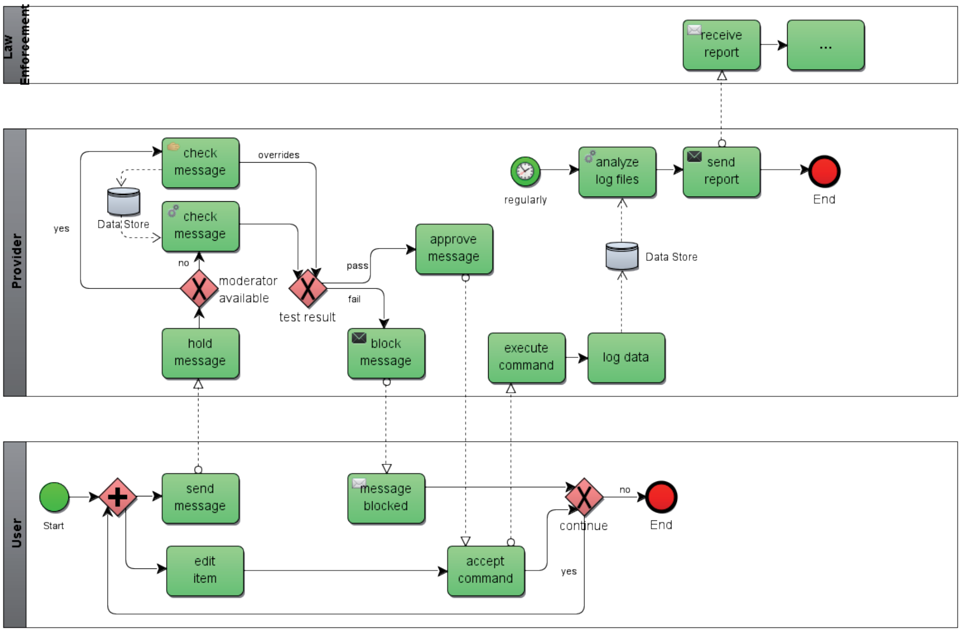


Figure 1 Communication between users can be subject of continuous monitoring. Moreover, all interactions can be logged and analyzed regarding suspicious activity patterns.

The process of automatically checking a message (including textual and visual content) is now explained in more detail in the following diagram.

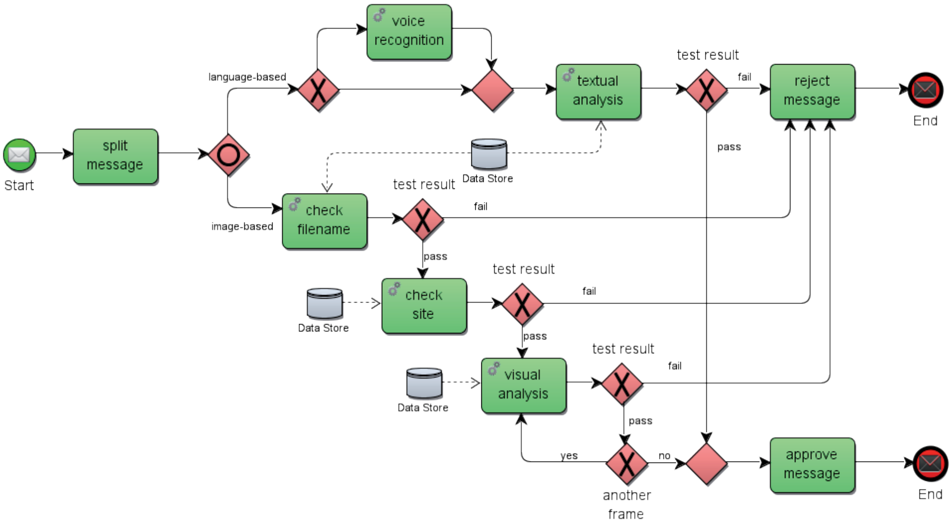


Figure 2 A message is split into textual and visual components, which are subsequently analyzed. Finally, a message will pass or fail these tests.

Up to now, the description of algorithms to analyze textual or visual content elements was rather vague. The next section provides in introduction to technical possibilities for this analysis.

4. Which mechanisms can we use for detection?

The description of image analysis revealed that a tradeoff between performance and accuracy of detection algorithms may become necessary, given the limited time for analyzing and rating messages in a stream. Moreover, technology asks for another tradeoff between accuracy and transparency, since transparent detection algorithms (i.e. those who come along with a reason for their rating) tend to be rather error-prone, and vice-versa. The next two sections present relevant approaches at either ends of this scale, followed by a third section describing a system architecture that integrates such algorithms and tools into a complete framework.

> *For the field of Cyber-Grooming, extensive empirical studies will be necessary in order to make pattern of offenders and victims explicit, before automated detection based on such rules can be applied.*

4.1 Rule sets

Rule-based systems are a well-studied approach to make knowledge of human experts explicit and interpretable by automated processing. Such an expert system defines a set of conditions on how to handle incoming data [12]. For this purpose, it consists of two kinds of machine-readable information:

- A knowledge base contains a set of information that was proven to be true.
- An interference engine describes a set of operations how this knowledge as well as incoming data can be transformed.

The expert system tries to infer new statements from this basis, with the final goal to conclude with a statement on approval or rejection of the message to be classified.

The benefits of such a solution are that every decision (in our case: on approval or rejection of a message to be classified as suspicious or not) can be justified in terms of the rules that have been applied. Moreover, there is experience from several application fields that are dealing with rule-based systems for several years.

However, there are some weak points. First of all, the success of this approach depends on the precision and completeness of given rules. This requires explicit modeling of knowledge in the respective field, which is a challenge where empirical data is still missing or not yet valid enough. For the field of Cyber-Grooming, extensive empirical studies will be necessary in order to make pattern of offenders and victims explicit, before automated detection based on such rules can be applied. Finally, complex rule sets make high demands on processing power. Current research on answer set programming [11] will help to tackle this problem.

These pro's and con's make rule-based systems more appropriate for textual analysis in the detection process described above.

4.2 Artificial neural networks

At the contrasting end of the scale, a well-known computational approach inspired by nature is available. Artificial neural networks imitate the structure and behavior of a brain in order to make a decision [2]. A number of switching elements (neurons) are arranged in a multi-layered architecture. They are connected with some preceding and subsequent switches following a given topology. Each connection is associated with a certain weight in order to strengthen or weaken the transmitted signal. Moreover, every switch has its own scheme to derive an output signal from the set of incoming signals. The overall output is calculated by the switches in the last layer. A network functions as follows:

- In an introductory learning phase, the artificial neural network is confronted with training data and the desired results of processing. The switching elements adjust the weights along their interconnections as well as their internal calculation schemes.
- In the working phase, the network can be confronted with new data that has to be classified.

Such an approach can be applied even to complex data or problems, since there is no direct equivalent of the problem description in the structure of the system. Thus, no explicit definition of rules is required, and the network (as well as processing time) will not necessarily grow with the complexity of the problem. Provided that a sufficient set of training data is available, proper functioning of the network can be established without expert knowledge. All calculations are available within few computational steps necessary for propagating the input data through the neural network structure.

At the other hand, the success of this approach heavily depends on the quality of training data and the training process. Thus, empirical data is required to some extent also for this approach. The main drawback of neural networks is that they do not provide any justification for their decisions. Thus, they can be used to prepare a recommendation or to generate short-term warnings, but not to create or collect evidence.

These pro's and con's make artificial neural networks more appropriate for visual analysis in the detection process described above.

4.3 Detection architecture

Following the discussions on how to analyze different types of content, how to handle private data, and how to integrate into the existing hardware / software structure of online environments, the following system architecture is proposed.

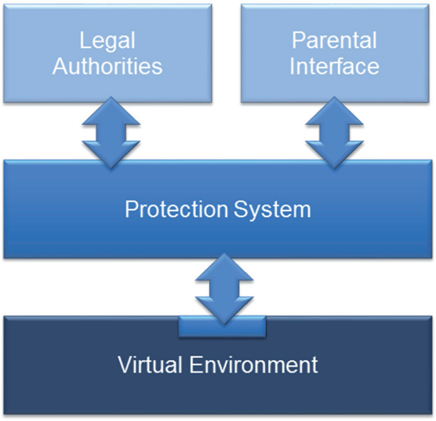


Figure 3 The proposed system architecture decouples police work and law enforcement from technological issues of single online worlds, while keeping privacy of users. Additional benefit is provided for parents to monitor their kids' online activities.

Officials from police, law enforcement, etc. do no longer need to tightly keep pace with technological progress. Rather, they can focus on monitoring, analyzing, and tracking criminal behavior.

Besides technical issues on where to handle which types of data, this layered architecture provides a strong benefit in decoupling legal authorities from system providers. Officials from police, law enforcement, etc. do no longer need to tightly keep pace with technological progress. Rather, they can focus on monitoring, analyzing, and tracking criminal behavior. A dedicated interface allows them to enter new case descriptions (i.e. patterns derived from their investigations) that are used to analyze upcoming activities in several online environments, independently from their technical connection.

On the other side of the system, interfaces to providers are established in order to integrate different online environments into the monitoring system. Currently, engagement like this is voluntary and very limited. Legal initiatives should force providers of online environments to integrate a plug-in of the monitoring system into their services in order to get a certificate as a child-safe place.

Another feature of the proposed system is an optional parental interface. Here, parents can get some possibilities to request reports on the activities of their kids. Of course, privacy should be considered, i.e. reports should be accumulated, and detailed information on dedicated activities should be given only in case of severe warnings.

Another added value from the cooperation of these parties is to integrate automated mechanisms for learning by feedback. Such an additional input can be decisions on messages by moderators, assessment of complex situations by law enforcement, and others more. Automated detection mechanisms must be able to improve their capabilities, as human supervisors would do. Such mechanisms of machine learning are subject of current research [17].

Another issue that technology cannot solve is to reason about the goal of a user. Does he/she act with criminal intent? Questions like these will always require human judgement.

It should be noticed that the generic approach described here is not specific to Cyber-Grooming, but can be transferred to several fields of crime, like economics, terrorism, sedition, and so on.

5. Conclusion

Computer science provides several means to automatically monitor and assess user activities in online environments. This article presented a rough overview, but further work is necessary to implemented the presented concept and mechanisms.

5.1 What we need

A basic requirement for all approaches presented above is the availability of observable behavioral patterns of offenders and victims with related probabilities of a criminal suspect. This must be specific for certain criminal activities as well as for certain national law. Thus, sophisticated empirical research in criminology (in relation to sociology and/or psychology) is necessary.

Another condition for successful realization of the solution presented above is the availability of interfaces to virtual environments, where plug-ins to the monitoring system can be entered. Since providers will not have intrinsic motivation to provide such interfaces, public pressure or regulations by law may force them to actively participate in protection of minor users.

5.2 What we can provide

As soon as detection mechanisms are installed, they can provide alerts on suspicious activities. They can be presented directly to player, but also to their parents, to providers of online environments, as well as to law enforcement.

Moreover, a monitoring system can help to collect evidence in case of a suspect or later trial. This can be information on the date, time and (virtual) place of an activity, on the person(s) involved, as well as on details on these activities. Given an official criminal investigation, these data can be forwarded from providers to law enforcement.

5.3 What we cannot detect

Independently of the technical implementation and surrounding conditions, there are some aspects that technology can hardly (if at all) provide. One of these is identity: Is a user the one he/she claims to be? The internet is based on the virtualization of identities. While biometrical data is reliable in local settings, digital transmission of identifying information is prone to manipulation. This is even harder is case of minor users. There are some mechanisms (like post-ident) to ensure that a user is above a certain age, e.g. for adult offers. These solutions are not capable to ensure that a user is below a certain age, since children typically to not have identifying documents. At least, their identity can easily be stolen by related persons. Another issue that technology cannot solve is to reason about the goal of a user. Does he/she act with criminal intent? Questions like these will always require human judgement.

References

[1] M. A. Anusuya, S. K. Katti: „Speech Recognition by Machine, A Review", Int. Journal of Computer Science and Information Security (IJCSIS) 06/03, Dezember 2009, S. 181-205.

[2] C.M. Bishop: "Neural Networks for Pattern Recognition", Oxford: Oxford University Press, 1995.

[3] S. W. Brenner: "Is There Such a Thing as 'Virtual Crime'?", 4th California Criminal Law Review, 2001, pp. 105-11.

[4] M. Brückner, C. Kanzow, T. Scheffer: „Static Prediction Games for Adversarial Learning Problems", Journal of Machine Learning Research (JMLR), Vol. 13, 2012, S. 2617-2654.

[5] K.-K. R. Choo: "Online child grooming. A literature review on the misuse of social networking sites for grooming children for sexual offences", Australian Institute of Criminology, 2009.

[6] F. Collins, D. McCormick: "Digital Selves: Lessons from Second Life", in Proc. World Conf. on Educational Multimedia, Hypermedia and Telecommunications (Ed-Media) 2011, S. 3405-3411, Chesapeake, VA, USA : AACE, 2011.

[7] X. Deng, V. Haarslev, N. Shiri: "Measuring Inconsistencies in Ontologies", in Proc. 4th Europ. Conf. on The Semantic Web: Research and Applications (ESWC '07), Berlin : Springer, 2007, S. 326-340.

[8] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Official Journal of the European Union, L 335/1, 17.12.2011.

[9] G. Ehrmann, U. Lucke, M. Mulder, T.-G. Rüdiger, T. Schulz-Spirohn, J. Storbeck, D. Woidke: "Protecting Children and Minors in the Internet: Perils of Cyber-Grooming in Virtual Worlds", Position Paper, October 2012. http://apache.cs.uni-potsdam.de/de/profs/ifi/mm/positionpaper-CyberGrooming-EN.pdf

[10] European Convention on Human Rights, ETS 5; 213 UNTS 221, Rome, 4 November 1950.

[11] M. Gelfond: «Answer sets», in: "Handbook of Knowledge Representation", Elsevier, 2008, pp. 285-316.

[12] A. Gupta, C. Forgy, A. Newell, and R. Wedig: "Parallel algorithms and architectures for rule-based systems", SIGARCH Comput. Archit. News, Vol. 14, No. 2, May 1986, pp. 28-37.

[13] S. Jacobsen, M. Mulder: „Dutch police, vision on youth and internet", in this issue.

[14] R. Koenen (Ed.): "Coding of Moving Pictures and Audio", ISO/IEC JTC1/SC29/WG11, Moving Picture Experts Group, März 2002.

[15] C. Krebs, T. Rüdiger: „Gamecrime und Metacrime: Strafrechtlich relevante Handlungen im Zusammenhang mit virtuellen Welten", Verlag für Polizeiwissenschaft, Dezember 2010.

[16] S. Livingstone, L. Haddon, A. Görzig, K. Ólafsson: „EU Kids Online", Final Project Report, 2011.

[17] M. Mohri, A. Rostamizadeh, A. Talwalkar: "Foundations of machine learning", Cambridge, MA : MIT Press, 2012.

[18] T. Morris: "Computer Vision and Image Processing", Palgrave Macmillan, 2004.

[19] Andreas Pfitzmann: „Contra Online-Durchsuchung", Informatik Spektrum 31/01, Februar 2008, S. 65-69.

[20] T.-G. Rüdiger: „Sexualtäter in virtuellen Welten", in this issue.

[21] N. Spirin, J. Han: "Survey on Web Spam Detection: Principles and Algorithms", ACM Explorations on Knowledge Discovery and Data Mining (KDD) 13/02, 2011, S. 50-64.

[22] Jörg Ziercke: „Pro Online-Durchsuchung", Informatik Spektrum 31/01, Februar 2008, S. 62-64.

About the author

Ulrike Lucke is Professor of Computer Science and head of the Complex Multimedia Application Architectures group at the University of Potsdam. Her areas of research are heterogeneity and interoperability of network-based architectures, including aspects of mobile and pervasive computing, especially in the field of E-Learning. Moreover, she is Chief Information Officer (CIO) of the University of Potsdam and thus responsible for strategic IT issues.

Protecting children and minors in the internet: perils of cybergrooming in virtual worlds

Georg Ehrmann, Deutsche Kinderhilfe e.V.
Ulrike Lucke, University of Potsdam
Manuel Mulder, Dutch Police
Thomas-Gabriel Rüdiger, Brandenburg Police Academy
Thomas Schulz-Spirohn, Prosecution Office Berlin
Jürgen Storbeck, Former Director Europol
Dietmar Woidke, Brandenburg Interior Minister

The EU has explicitly admitted to making the Internet a safer place for kids and minors[1]. The discussion in the EU on protecting children is finally focused on the question to just block or completely delete harmful websites. This is not targeted to online environments (like virtual worlds, browser games, online apps), but is stuck to an out-dated content-oriented (not: communication-oriented) view. Kids primarily explore the internet by starting to play games, not by surfing the Web[2]. Those online environments are especially attractive because of their possibilities to interact and communicate with other players (like shared game experience, chats). There are certain offers with a design and game mechanism that is particularly suitable for children, where they are especially exposed to enter close emotional relationships with others. Besides other legal issues, this is intensively exploited by pedo-criminals in a targeted manner[3]. Such initiations of sexual interactions with minors are called Cyber-Grooming[4].

This important, but not yet sufficiently covered topic was primarily addressed by the symposium "Protection of Children and Minors in the Internet – Perils of Virtual Worlds" on 19 September 2012 in Brussels. Starting from a criminological overview of the phenomenon, aspects of law, society and IT for protecting kids and minors against Cyber-Grooming have been considered by respective experts, and first experiences with virtual police offices in an online game for kids have been presented. In the following, the political consequences have been discussed with representatives of EU commission and parliament. All participants agreed that the Internet is an important part of today's media reality, and that providing related skills as well as an adequate protection of minors are a central goal of our efforts.

As a result, there were identified short-comings of law, investigation, prosecution, and prevention; and a first catalog of possible countermeasures was gathered. Among others, a new age rating (age levels,

[1] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Official Journal of the European Union, L 335/1, 17.12.2011.

[2] S. Livingstone, L. Haddon, A. Görzig, K. Ólafsson: „EU Kids Online", Final Project Report, 2011.

[3] Susan W. Brenner: " Is There Such a Thing as 'Virtual Crime'?", 4 Cal. Crim. Law Rev. 1, 105-11, 2001.

[4] Kim-Kwang Raymond Choo: "Online child grooming. A literature review on the misuse of social networking sites for grooming children for sexual offences", Australian Institute of Criminology, 2009.

criteria, and responsibilities), an adequate media-related instruction of kids as well as training of other involved players (teachers, police men, state attorneys, system providers), and a general sensitizing of the society for the perils of interaction and communication in the Internet were proposed. Moreover, the development of technical means to detect and block suspicious activities in online environments were discussed, which need to be balanced between safety and privacy. Further efforts to elaborate and implement the mechanisms mentioned above will follow in the near future.

Imprint

Publisher: Rainer Grieger
President of the University of Applied Science of the Brandenburg Police

Editorial Staff: Thomas-Gabriel Rüdiger, M.A.

Fachhochschule der Polizei des Landes Brandenburg,
Bernauer Straße 146, 16515 Oranienburg, Germany
Phone 03301-850-2501
Fax 03301-850-2509
E-Mail fachhochschule@polizei.brandenburg.de

ISSN 1865-1062

Printed by University of Applied Science of the Brandenburg Police

Editorial Deadline: 30. April 2013