Winter '16

Online games as risk generators for children and adolescents –

Analysing risk factors in gaming environments

Diana Selck and Thomas- Gabriel Rüdiger

Table of content

1 Introduction

Breck Bednar, a 14-year old boy became victim of a cybergroomer[1] on the Internet. He met his perpetrator in a secretive online game forum in which he was invited due to his talent. Breck was an average adolescent, with a good relationship to both of his parents, good grades, overall a smart kid interested in technology. He enjoyed playing online games, meeting and making new friends online. And this is how he met Lewis Daynes, a boy supposedly 17-years old, running a well off computer engineer firm. Breck spend increasingly time with Daynes online. After awhile this became evident by the way Breck started behaving, not willing to finish school homework or do chores or accept parental measures in order to limit his Internet consume, and thus separate him from the voice that came constantly out of his headphones. His mother became worried, approached other parents and teacher in order to receive some advice. At the end, she called the police, describing the new online friendship of her son and expressing her concern that she had towards the stranger, whom her son talked to on a daily basis. She was worried that her son might be groomed online. The police, teachers and other parents tried to convince Breck's mother that this is a normal behaviour of a 14-year-old boy, which would pass, eventually. At the end Breck's father suggested to meet with Lewis Daynes in the real world in order to make sure that he is who he claims to be. The meeting never took place. Instead Daynes claimed to be very sick and therefore would soon need someone to take over his company. At the end, Breck pretends to hang out with one of his real friends but instead drives to Daynes' apartment to finally meet his online friend. In the night of the 17th of February in 2014, Breck was stabbed to death, the court later ruled that the actions were sexually or sadistically motivated and conducted by the 19-year-old unemployed Lewis Daynes (Elgot, 2016; Moore, 2016).

The Internet and the usage of platforms to communicate, exchange information, meet people online as well as play online games are ubiquitous. Especially children[2] of today grow up with information and communication technologies (ICTs), using

---

[1] Online grooming or cyber grooming can be understood as sexual harassment of children through online-based programs as well as the establishing contact with a child through the Internet with the intention of sexual misconduct. This phenomenon is called cyber grooming, the person assaulting is most often termed as an online predator (Rüdiger, 2015a).

[2] Children in this study will be considered within the legal term of a child under the German penal law, which defines children until the age of 14.

them in a wide range of activities. Online gaming claims one great part of leisure activities of children and adolescents. Online games can be defined as a "[…] digital game that needs a live network connection in order to be played. This includes not only games played on the Internet, but also those played online through consoles[3], across mobile phones or via peer-to-peer networks." (www.pegionline.eu).

In Germany, 56 per cent of the 6 and 7-years old children play online games occasionally (Kempf, 2014). According to the "Bundesverband Interaktiver Unterhaltungsmedien" (BIU), already 26.4 million of the German population plays online games (BIU, 2014).

Consequently, children and adolescent have been introduced to online gaming and the interactive nature of virtual worlds. Nevertheless, online games also produce risks for this specific user group. In media, several cases regarding high amounts of telephone invoices and the billing of surprised parents by telephone provider have been published. In these cases, children often did not realise that the proclaimed free-of-charge-games had a billing function (e.g. in-game purchases) within the applications of the games and thus spent hundreds or thousands of euros with virtual purchases.

Research regarding the risk of sexual online perpetration as well as financial losses in online games for children and adolescent are especially in the German-speaking areas almost non-existent (Rüdiger, 2016). Existing studies barely considered online games as platforms to interact and communicate with strangers. Consequently, an analysis of possible risks is imperative.

In this study[4], data from thirty-two online games of mostly German online game providers was conducted[5]. Nevertheless, due to the nature of the Internet, German online gaming providers are accessible from all over the world, only restricted by Internet access and regulations of IP inspections.

The purpose of analysing online games underlines three important implications.

First of all, the age restriction regulations of each online game. Here, the first obstacle to overcome was that no universal age regulations as well as age recommenda-

---

[3] Consoles are generally considered when talking about online risks in online games. This study has only focused on browser games accessible via browser and mobile app games accessible via phone and tablet devices. Consoles are generally accommodating the same online risks considered in this study.

[4] The current study concentrated on Germany or a German-speaking field as the examination field. This is important when considering legal frameworks and definitions, e.g. in the area of child and youth media protection and age recommendations.

[5] This does not imply that game provider and servers are located in Germany

tion could be found[6]. Online games are provided on different platforms, for the analysis the focus was on downloads such as mobile games from the Google Play store (Android), iTunes (Apple) or games accessible through the browser such as free-to-play (F2P) browser games. This was also one reason why different actors were involved for age recommendations of games and thus irregularities in age regulations could be found.

Secondly, it was focused on payment options within online games to find out how many verification or locks would be faced before one would be allowed to spent real money. And at last, the possibility of communication within the games were analysed. Here, the focus lay on the accessibility to children and adolescent. How easy would it be to talk to any stranger within an online game?

From a criminological perspective, these questions are important in order to identify the risks of online offences such as (sexual) online perpetration of children and adolescents in online games as well as enable prevention measurements to prevent tragically endings such as the Breck Bednar's case provided. In the future, security agencies should be able to identify online grooming and act accordingly in order to prevent crimes against children and adolescents.

2 Risk factors in online games

2.1 Forms of online games

Many different forms of online gaming exist, which to a certain degree depend on a functional Internet connection in order to play with other players. In this paper it will be focused especially on online games in which players are able to meet people, join gaming groups and other forms of alliances in order to communicate with each other. Games, for example massively multiplayer online role- playing games (MMORPGs) and massively multiplayer games (MMOGs) are widespread and two of the most popular types (Yu-Wei-Chang, 2015; Williams & Skoric, 2005) of games

[6] Generally, Germany provides two legal frameworks when considering age regulations and recommendations. First, the youth protection legislation (in German: Jugendschutzgesetz), which regulates age recommendations regarding disk-based programs, e.g. computer games that can be purchased on a physical disk. In this case, the USK (in German: Unterhaltungssoftware Selbstkontrolle) implements the age classifications. Regarding online games that do not need a physical disk but are accessible through the web browsers and mobile Apps and thus only need an Internet connection, no comparable standard exists. Online games are held under the Interstate Treaty on the protection of minors (in German: Jugendmedienschutz Staatsvertrag – JMStV), which does not prescribe age recommendation for online products towards the youth protection legislation (also see Rüdiger, 2016).

played online with genres as *casual*, *strategic, first-person-shooter (FPS), sport* and *action*.

MMORPGs are characterised by predominant medieval or future-oriented fantasy worlds in which gamers act through avatars. Avatars are faced by challenges and gain strength with each mastered task. Managing game stages and levels is highly interactive and involves other game members as well as group mechanisms. As Ballard and Welch (2015) state, most online games allow for social interaction, leading to organised alliances or groupings known as guilds, clans and tribes, which collaborates with a small but still unknown group of people (ibid.; Ducheneaut et al., 2006). Ducheneaut et al. (2006) characterise guilds as places in which most of a player's relationships are formed. Guilds, clans, tribes and other forms of alliances play an important role and show how easy it is to meet strangers online and form relationships on the basis of the provided information given by players themselves. Both, adolescents and adults are equally engaged in these forms. Until today, MMORPGs are very popular games in the digital games market, offering a platform for virtual communities and a basis for social interaction (ibid.: 472f).

Some games involve group mechanisms that are depending on the length of a game provide incentives for users to join groups instead of playing individually. Alliances are characterised by clear work distribution and hierarchies, which can have an advantageous effect. Participants of these groupings are in a constant development of their avatars and virtual realms.

Generally, online games can then be differentiated in their utilised business models. Pay to play (P2P) games such as World of Warcraft, which has to be purchased for a certain amount of money before it can be played. In many cases, the user has to agree similar to a form of monthly paid subscription. In opposite of this model, stands the business model of free to play (F2P) games, which suggests that the game is not bound to any costs and is free to purchase and download. The F2P games finance themselves through so-called in-game purchases or in-app purchases. In-game purchases are purchases for virtual items or gain of game advantages. In many cases, virtual items will be purchased with an in-game currency, which often inherits a playful title such as coins, elixir, gems, sunflowers, etc. These virtual currencies can either be acquired by rather lengthy game operations or with real money. If one individual gamer is not able to participate for a certain amount of time, disadvantages will show expeditious. In order to be not left behind and remain in the

lowest hierarchy, the user must push his or her developments. One appealing way of upgrading to stages that others might have reached during a time of the users absence could be with real money and thus in-game purchases. One of the most well known online games – Clash of Clans from Supercell - generates up to 5 million Dollars per day for purchasing virtual items (Diaz, 2015).

2.2 How online games need to be considered as possible risk generators

Online games have become a big part of children and adolescents leisure time and thus can put their users at risk to become victim of harmful behaviour, criminal activities, immense financial losses and gamecrime (Krebs & Rüdiger, 2010; Rüdiger & Pfeiffer 2015). Gamecrime will be elaborated more deeply in the following section 2.3. The amount of time children and adolescents spend in online games is also underpinned by several studies. A German study called “Jugend, Information und Multimedia” (JIM) conducts every year a study documenting the usage of information and communication technologies (ICTs) and media competence of 12 to 19-year-old adolescents. According to the study, 25 per cent (n= 1,200) play online games on a daily basis (Medienpädagogischer Forschungsverbund Südwest (mpfs), 2015: 11). Twenty-two per cent of the interviewed adolescents are playing online games several times a week (ibid.). A similar finding provides the report of EU kids online from 2014. According to the report, 28 per cent of 11 to 16-year-olds play online games with other people on the Internet. Back in 2010, only 16 per cent of the questioned adolescents were playing games online (EU kids online, 2014: 11). Another study, namely getsafeonline (2015), analysed parents perspectives (n= 2,000) about their 5 to 18 years old children and adolescents and their online behaviour. They found out that one third of parents feel that they do not really know about their kid’s online gaming activities. Sixteen per cent of the parents are aware that gaming platforms can increase the risk of being bullied or verbally abused (getsafeonline, 2015). Even though, the study is right at the point of asking parents how much they know about their children’s gaming activity; the study does not consider risks of online perpetration and cyber grooming or the risk of financial losses.

In the majority of these studies, it is not clear how online games are understood and considered in their analyses. The JIM study (2015) found out that every second adolescent plays ‘digital games’ in their leisure time on a regular basis (Jim, 2015: 12). JIM understands digital games as games on the computer, consoles or games in the

Internet (ibid.). It seems that mobile games via applications (app) are not considered at all, even though online games are increasingly played on mobile devices. According to statista (2015a) the weekly time spent by children between the ages two and 17 playing mobile games has increased from 5 hours weekly in 2011 to 7 hours in 2013. In December 2015, the most popular App store category by share of available apps was gaming with 22.49 per cent (statista, 2015b). Gaming apps are the most popular app category based on availability and top-grossing iOS gaming apps that generate more than 1 million U.S. dollars per day (ibid.). According to getsafeonline, the most popular devices to play games online are tablets, 62 per cent of the children use this device to play online games. This is followed with 47 per cent of children and adolescent using their parent's mobile phone to play games (getsafeonline, 2015).

It is significantly important to consider all forms of online games and clearly distinguish between them in order to understand the risks they can pose. For example, there are online games that can be considered as games, which are offered on online platforms such as Steam[7], which can be played online, but include no possibilities for communication and interaction with other gamers. These forms of online games do not face the same online risks that can be experienced with games that provide an anonymous way of communication and interaction with strangers. It is noteworthy, that other risks exist, which will not be considered in this paper. Among others risks such as violence, exposure to pornography and extremism can occur in online games (Krebs & Rüdiger, 2010; Rüdiger & Pfeiffer 2015).

Another issue that will be considered is the integration of various paying methods in online games. Therefore, this study will focus on games with communication and interaction possibilities as well as payment options in online games. It will be particularly focused on F2P browser games, which can be played through the browser or mobile application (App) and client.

In general, F2P browser games can be easily accessed with a functional Internet connection and the fitting hardware such as laptop or computer. App games are accessible through mobile phones and tablets devices and can be downloaded on specific platforms such as Google Play store, Windows store and iTunes. Another

[7] Steam is an online platform that can be installed to play pay-to-play computer games and free-to-play online games. (http://store.steampowered.com/about/)

form of an online game can be operated through a client. By downloading a client, the gaming experience can be better than playing a game in the browser due to faster processing and a stable connection.

2.3 Gamecrime

Characteristically, crime arises from interaction between two individuals. Participants of this interaction do not always have to be aware of their participation, but it takes place nevertheless. Consequently, a child or any other game member is often unaware of interacting with an offender and thus does not report the interaction or files a complaint. On the other hand, criminal activity can evolve out of an aggressive confrontation between two individuals in which both participants are aware of the situation. Consequently, whenever two individuals interact, actions and decisions take place. Why would this be different in virtual worlds such as online games? Appropriately, criminal actions in online games are called gamecrime (Krebs & Rüdiger, 2010; Rüdiger & Pfeiffer 2015). Gamecrime can be understood as forms of crime that erupt in online games or gaming environments such as online game platforms as Steam, PSN or Xbox- Live (ibid.). It inherits various forms of crimes depending if criminal offences are in-world (within the game) or out-world (outside of the game). Out-world offenses are crime forms that aim to interfere from outside into game mechanisms, e.g. gaining access to login data or attempts to hack game accounts. In-world crimes are offences, which result from communication and interaction of the players within the game. This area of gamecrime is particularly of concern in this study, questioning the issues of ubiquitous and anonymous interplay of adults with children in online games.

This issue is described more thoroughly in a blog thread written by Rüdiger (Rüdiger 2015a). In his article he compares the online gaming environments with an offline playground. It is scrutinised how the presence of online groomers in gaming environments seem rather ordinary and are not sufficiently questioned. In comparison, the presence of a stranger and possible perpetrator on a public playground would lead to some sort of action. The article argues further: “Imagine a playground where your 10-year old son or daughter is playing and a 35-year old man walks up and begins playing with your child.” The reaction to this situation would be vigilant if not aggressive-protective. Parents would want to know who this stranger is and which intentions he or she has of approaching their child, pretending to be a like-minded 10-year-old. Such meet-ups of children or adolescents with adults are nowadays

ubiquitous in the online gaming landscape (Rüdiger, 2015b). Consequently, one immensely prevalent risk for children and adolescent is the danger of meeting an online perpetrator. Breck Bednar's case is only one of many in which the victims are not aware of the risk their so-called online friends could pose. Breck became victim of an online (sexual) perpetrator, leading to an offline face-to-face meeting. In their study, Cheong et al. (2015) analysed predatory behaviour in game chats and thus defined sexual predation with the characterisation of *age disparity*, and hence an adult who chats with a minor in an *inappropriate intimacy* (ibid.:220).

Another risk that is until now under-researched is the risk of financial losses. Especially children, who play online games on mobile devices, have in the past spent unknowingly great amounts of money with in-app purchases. In-App purchases are purchases made from within a mobile application (www.webopedia.com). In some cases Apple has decided to refund parents of great financial losses (Lipka, 2014). At the presence, there exist no regulation for unwillingly purchased virtual items made by children and adolescents. In Germany, the legal situation regarding similar cases has not found a legal consent yet. In the past, German courts have ruled differently in cases like this, for example the regional court of Saarbrücken commented on a case in which parents had to pay a bill of 2.800 Euro. In this case the 12-year-old son spent 2.800 Euro for virtual items in an online game. As e result, the court expressed that the whole system of these games enabling children to play (and pay), is close to a violation of moral principles (Schulzki-Haddouti, 2014; Sevriens, 2011).

Consequently, parents cannot rely on the current legal situation or court ruling, which is far from clear and thus can only hope for the goodwill of platforms, which provide games such as iTunes by Apple or Google play store.

2.3.1 Sexual perpetration in online games

One of the main risks analysed in this paper is online sexual perpetration in games through Cyber Groomer[8]. In the study of possible chat room regulations, Joint (2003) reasons that paedophiles using chat rooms to increasingly target victims and lure children into potentially dangerous situations. He further argues that children

[8] In the German-speaking area, one general term has been established when speaking of sexual harassment of children through online-based programs as well as the establishing contact with a child through the Internet with the intention of sexual misconduct. The phenomenon is called cyber grooming, the person assaulting is most often termed as an online predator (Rüdiger, 2015a).

enjoy the exciting opportunity to flirt and chat to others in their own age. This becomes problematic due to the anonymity of the Internet, children and adolescents cannot be sure of the proclaimed age of their fellow players. "By creating a false identity, lying about their age, 'grooming' their potential victims and then arranging to meet them in person, children easily become sitting ducks for child abusers." (Joint, 2003: 44). While admitting to the possibilities of grooming children in chat rooms, Joint does not consider online games as potential platforms for these criminal activities. This might be due to the date of the year in which the article was published. In 2003, online games might not have been recognised of an equally used platform by children and adolescents as well as child abusers than the more common place such as social media platforms. This is also evident in the research of Sylvia Kierkegaard from 2008. Even though, she considers the Internet as a place for positive and negative opportunities and thus recognises online grooming and sexual perpetration as a growing issue, Kierkegaard does not consider online games as such. In her analysis, Kierkegaard (2008) states that among privacy issues and exposure to harmful content such as pornography, grooming and encouragement of harmful behaviour, these issues have become problems of an international wide-ranged nature. She identifies chat rooms, blogs, email exchanges, mobiles and other social network sites as places in which deliberate grooming exploitation of a child by an adult takes place (ibid.) and thus covers various meeting points for victims and offender but not online games specifically. Nevertheless, Kierkegaard (2008) considers the virtual world and the Metaversum of Second Life and age play. Second Life is the largest virtual world created entirely by its users (www.secondlife.com). Children age play is an in-world sexual activity between a child avatar and an adult avatar that engage in simulated sex (Dirry & Rüdiger, 2015). With the issue of age play, a whole new discussion emerges of rather simulated sex and online rape should be considered as criminal activity and thus illegal (Kierkegaard, 2008: 44). Once again, the reason why Kierkegaard is not considering other online games could be that in 2008, online games in general were not (yet) viewed as possible grooming places. Even though, according to Rüdiger (2015) online games have established in the past 15 years, research might take some time to recognise the issues at stake. While Joint considers the rather technical and legal issue of criminal reliability of the Internet service provider (ISP) itself, Kierkegaard focuses on a national as well as international legal ground in order to combat cyber crime against children. Nevertheless, both argue that nearly everywhere legislation is still playing catch-up to the advanced and sophisticated techniques of child abus-

ers (Joint, 2003: 47; Kierkegaard, 2008). Joint (2003) follows this and states: “After all, in real life, there are places where parents can leave their children quite happily and they would be safe to play unsupervised, and there are others where they would never dream of leaving children on their own. The same rule should apply in cyberspace.” (ibid.: 48). Kierkegaard agrees that technology develops faster than law, and thus law need to be strengthened to address challenges like this (Kierkegaard, 2008: 55), and therefore catch up with technological advances.

The risk of meeting online perpetrators also becomes evident when looking at the recently published data from the United Kingdom. English Police noticed between 2013 and 2016 that 400 children were either abused or became victim of cyber grooming over the Internet, more specifically through social media platforms. Interestingly, one of the main platforms that provided a meeting point between children and offender were online games. Police stated one game in particular, Clash of Clans, which has already received law enforcements attention lately. The game provider of Clash of Clans namely Supercell has as a reaction of the statement of the police announced that the game’s terms and condition exclusively recommend the game only for the age 13 and older (Supercell, terms and service) and thus only children and adolescents should download it (Scheerhout, 2016).

In fact, if one takes a closer look, the game provider Supercell recommends the game for the age 13 and older, while Google play store classifies the game for age 0, iTunes for the age 9 and Google search results as well as computer-related blogs recommend the age 6. This underlines the issue of the irregularities of age recommendations.

2.3.2 Financial loss

Financial loss for children and adolescents is one of the considered risks of this paper. Due to the absence academically research, media reports will be considered regarding cases of financial losses. Financial losses in this case, will be understood as unintentionally high expenditure of money within online games. In all of the cases, neither children nor parents were aware of spending real money while purchasing game money such as coins, jewels, weapons, lives or other virtual items. The cases here presented are from different countries, underpinning once again the borderless and international nature of this issue and the lack of an international legislation. Until today, cases that will be stated below were only handled by the gaming

companies on the basis of goodwill, and thus make it evident that regulations are needed.

Case 1: United Kingdom

In the UK, three children have summed up their parents credit card bill to 350 pound by playing two games, which were free to download (*Clash of Clans* and *DragonVale*). The children purchased "virtual gems". The mother argues: "They think it is virtual money in a fantasy land […]" (Martinson, 2013). Jane Martinson is pointing her finger to Apple, who in the past has refused to cancel the thousands of pounds spent by other kids, citing parental responsibility and pointing out the fact that its products all contain password locks to prevent unwanted or accidental purchase. Martinson wonders if these in-game purchases for free games are just another way of exploiting their children (ibid.).

Case 2: Belgium

A 15-year-old boy spent approximately 37,000 Euros on gold in the free-to-play game called *Game of War: Fire Age*. The boy from Belgium bought in-game gold with his grandfather's credit card. He was only able to use the credit card information because he helped his mom purchasing an e-Book. Both, the mother and the grandfather were not aware that the boy linked the credit card information to his own iTunes account (http://www.nieuwsblad.be, 2014). In the article it is not stated whether the boy knew what he was doing or not, still the mother and grandparents are left with a great amount of debts.

Case 3: Sweden

In Sweden a free-to-play online game cost a family 60,000 SEK. The 9-year-old son played in a time period of two weeks the free to download game *Clash of Clans*. The boy spent two weeks at his grandparents place asking his parents for permission to play a free game during that time. When the first bill of 21,000 SEK arrived, the parents tried to investigate why such a great amount was charged from their credit card. Only one day after, the bill mounted up to 49,000 SEK. When the parents contacted Apple for help, the total credit card bill was 60,000 SEK. The parents still await answer from Apple and hope for a refund (Svahn, 2015).

All of the three cases have shown that proclaimed free-to-play games or free to download games are not as free of costs as they seem to be at first glance. Google

Play store or Apple iTunes, which are providing platforms for Android or Apple devices to download games, have responded to these issues by introducing password locks and providing safeguard options. However, Apple still requires the linkage of a credit card to any created iTunes account, especially after using the iTunes store or App store for the first time (Apple support, https://support.apple.com/de-de/HT203905). Without an iTunes account and thus an Apple-ID, Apple devices are not able to purchase any items. Consequently, every functioning iPhone or iPad or other Apple-driven device is linked to a credit card or other payment options. Furthermore, in-app purchases are only one of many options to pay for virtual items. Free-to-play browser games, which are played on a computer or laptop, have a wide range of payment options.

Case 4: Germany

According to the law firm Hollweck, a mother of a minor (under the age of 14) received a shocking high telephone bill of the total amount of 4,700 Euro. Google Play store and a provider called BOKU charged her due to purchases made in online games. Online games such as *Clash of Clan*, *Rayman Jungle Run*, *The Sims* were listed on the telephone bill. Clash of Clan was one of the games that the under-aged son has spent the most in. All of the games were free to download but offered in-game purchases, e.g. through telephone and text messaging or provided credit card details.
As the last case shows, other payment methods than paying by credit card are possible in online games.

One of a rather easily accessed method is the payment method by phone. In the case of paying by phone, children and adolescents only can dial a 0900 – number, which charges the individual telephone provider within the next monthly bill. In case 4, the telecommunication provider Telekom was charged by the third parties Google Play store and BOKU. Telekom in turn, charged the mother with the total amount of purchased virtual items (Holloweck, 2014).

3 Methodology

This study was conducted by means of a multiple approach of qualitative methods in order to analyse certain levels of risk factors for children and adolescent in online games. Qualitative research was more fitting due to the insights qualitative methods can provide of the research subject (Flick, 2000). In this case, the research was conducted in the Internet in which the Internet is considered as a) a medium of communication and b) as a context of social construction (Markham, 2004; Hine, 2005). The Internet as medium for communication provides new channels of communication with other individuals or groups. On behalf of the Internet as a context of social construction, Markham (2004) states that the Internet is a unique discursive milieu in which the researcher can witness and analyse structure of talk, development of relationships and communities (ibid.: 97). Therefore, the Internet offers the qualitative researcher many ways of observing and/or for interaction with participants (ibid.). Hine (2005) agrees and names the online world a fruitful field for researchers and thus suggests that the online context can be claimed as ethnographic field (ibid.: 8). A consistent discussion can be found of whether new research methods are required for new online settings in the virtual ethnographic field site (Emmison, 2004; Hine, 2005; Williams, 2007).

Mann and Stewart (2000) found out that the main tools for data collection in the Internet favoured by qualitative researchers are still the conventional ones such as interviewing, observation and document analysis (ibid.: 65). Even though, ethnographic fields can be found in new online settings, existing methods can still be applied to the field.

The qualitative method chosen in this study was participant observation. According to DeWalt and DeWalt (2011) the goal of participant observation is to establish an understanding of the nature of phenomena. Other advantages in participant observation are that this method provides a lower level of interaction with the researcher and a stronger emphasis on documentary analysis (Man & Street, 2000: 84). According to Foster (1996), observational techniques can also have advantages over interviews. First of all, information can be recorded without relying on others; observers may see the familiar as strange, noting features of environments or behaviour that participants may not be able to see (Man & Street, 2000: 84). Additional advantages are that the observation can take place over a longer period of time and therefore observations allow access to information about people who are otherwise

too busy, deviant or hostile to take part in research (ibid.). Also, collected data and its interpretation might have an enhanced quality; making this method both data collection and an analytical tool (DeWalt & DeWalt, 2011: 10).

In this study, risk factors for children and adolescent in online games were the primary research subject. In order to identify different levels on risk factors, participant observation was used for only one purpose: to observe activities and interactions, people and thus gamers as well as gaming mechanisms. According to Spradley (1980) participant observation has generally two purposes: 1) engagement and 2) observation. He argues further and states that the participant observer will experience both insider and outsider simultaneously (ibid.: 57). Back in 1980, Spradley used the example of a poker game, while participating in poker games and thus identifying the observer as insider. But at the same time experiencing him and the other players as objects from an outsider perspective (ibid.). The same dual participant observation method was applied to this study. Even though, at first glance engagement and therefore a dual participant observation were not intended at first. In order to become an insider of online games and obtain data, a registration and creation of an avatar was necessary. Therefore, engagement in this case was not to make contact with other players and thus leading to interviews but engagement was mandatory in order to identify game mechanisms such as registration processes, observation of chat functionality and means of various payment methods.

As participant observers, avatars were created, villages set up, clans, guilds and other association were joined and it was participated in group-activities, e.g. clan wars and communication with group members. Simultaneously slipping into the insider and outsider role as a participant observer.

3.1 Investigation period

The research was conducted between December 2014 and March 2015 and last checked of its validity between September 2015 and November 2015. The total of 32 online games were tested, most games chosen from well-known online gaming companies from Germany. Approximately 70 hours of game time, including systematic observation of game mechanisms such as registration processes, age recommendation, enablement of chat functionalities, interaction between players and payment options.

3.2 Choosing the research subjects

Free-to-play games were chosen due to the low cost expenses. Not only research is limited with the need of maintaining costs low but also children and adolescents have in general a low budget and thus might use these games more frequent.

The games tested were all free to download and mainly browser games and hence played in the browser without any further steps to install or download applications. Yet, some of the games were also available in mobile app versions, which were tested on smartphone or tablet devices. Others had to download a client first, which the game provider offered to download from the games website. That is why four classifications of the tested games were made. Noteworthy, all of the tested games classified themselves through their enablement of an Internet connection and provision of interaction and communication ability within the games. The first type of the tested games was *browser games.* Secondly, games that could only played via applications, namely mobile games*.* Third, games that were offered as a browser game and could be played on a mobile device via an App, namely *browser game and mobile games*. And last, games that were played via clients, and thus called *client games*. In summary, the amount of games that were tested within their classification was browser games (20), mobile games (4), browser games & App (5) and client games (3). All tested games and the associated game companies were anonymised so that no disadvantages will result from the study's findings. Due to the time consuming task of testing online games, the authors were not able to test every free-to-play online game that is on the market. It is noteworthy to point out that the selected games only provide a temporarily insight. Each year, new online games are released on the market that might replace old games or illustrate a completely new set of online gaming with different challenges and risks.

A total of four online gaming companies were tested and four individual games, which have their origin in Finland, Denmark and Germany. Game company 1 (GC1) provided eight games (game 1-8) with reliable data that was comparable to the other companies. Game company 2 (GC2) supplied this study with eight games (game 9-14). Six games (game 15 – 20) could be tested from game company 3 (GC3) and eight games (game 21- 28) gave enough information to include in this study from game company 4 (GC4). Additionally, four individual games chosen by their popularity were tested as well. Each was chosen from a different game company and thus is named the GC5, GC6, GC7 and GC8. The four individual games are therefore

according to their company continuing with the game number game 29, game 30, game 31 and game 32. Some of the individual games were already known to have had experienced cyber grooming cases. Noteworthy, games that enable online communication always inherit the risk of sexual harassment (Rüdiger, 2016; Sauerbrey, 2015).
In order to identify possible risks for children and adolescents in online games, three main focuses were set, namely age recommendation, payment options and chat functions.

4 Age recommendation

4.1 Background

Age recommendation[9] is one important aspect in managing the risk for children and adolescents in online games. Age recommendation can guide parents, legal guardians and children themselves of whether the games are classified for their age or not. Until today, there is no verification regarding registration processes in online games. A valid email address and a password are sufficient and are the only requirements needed to fulfil registration conditions of the tested online games.

One obstacle to overcome was the difficulty in finding one clear age recommendation for each game. Interestingly, many of the tested games were classified for the age of 12 and under by the official institution of USK (see also diagram 1). Since 2015, USK is also responsible to classify age recommendations for games on an international level within the framework of the international age rating coalition (IARC) for all forms of game providing platforms including the App store and Google Play store as well as Windows store (http://www.usk.de/iarc/). Nevertheless, this still remains only an age *recommendation* that can be voluntarily followed or not. Until today, there is no legal regulation or age recommendation that is either embedded in the youth protection legislation or in the Interstate Treaty on the protection of minors.

Among the tested gaming companies only one game provider stated in its terms and conditions that players must be 18 years old regardless of age recommendations

[9] This study focused within the framework of official age recommendations defined by USK. An similar analysis regarding age recommendation in an European (Pan European Gaming Systems (PEGI)) or international context would be fruitful and interesting to compare with national results.

from others such as USK, computer related blogs or other search results (see also appendix p. 35ff).

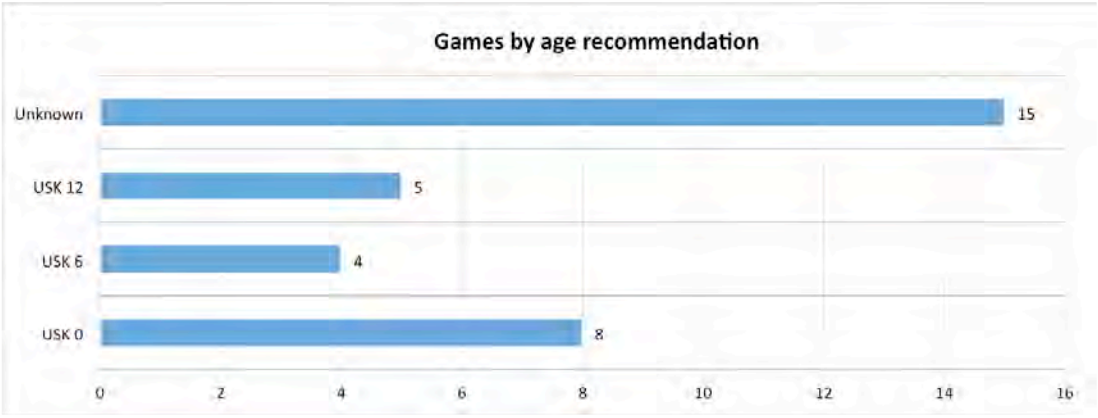

Diagram 1: Age recommendation of game provider and online game platforms

4.2 Methodological approach and results

The first issue was to find out, if one of the tested online games recommends or even restricts the access to the game. Consequently, each game was thoroughly browsed through regarding age recommendation. In order to do so, legal *terms and conditions were read* (in German: AGBs) and each game website (if existing) was searched for signs such as the German USK would provide. If the game website itself did not provide any recommendations, it was checked on the homepage of USK (usk.de) and the search function was used to find the games individually. If still no result was visible, the search engine Google was utilised to find age recommendation for a specific game. When results were shown from an unknown computer-related blog page, it was double checked with other search results in order to conclude which age recommendation for the desired game was applicable. Out of the total of 32 tested online games, age recommendation were drawn from either the game itself, the USK website, Google search or the websites of the games, and thus often three different age classification were provided. Other than that, identifying a recommended age group for each corresponding online game was next to impossible. Resulting from there, eight games were recommended for the age 0 (USK0). Four games were classified for the age of six and older (USK6). And five out of 32 games were recommended to play at the age of 12 and older (USK12). For fifteen of the tested games, finding a reliable age recommendation was not possible (see also diagram 1).

The non-existence of a universal age recommendation makes it rather difficult to move through the jungle of gaming blogs, official age recommendation sites as well as websites of gaming companies. In four cases, age differences between each recommendation were so great, that a sufficient conclusion of which age restriction should be applied was not possible.

Similar results can be found for another online game. In this case, the game provider does not recommend any age on the game's website, while iTunes recommends the age 12 and Google search produces the age recommendation of the age 6 (see also diagram 2).

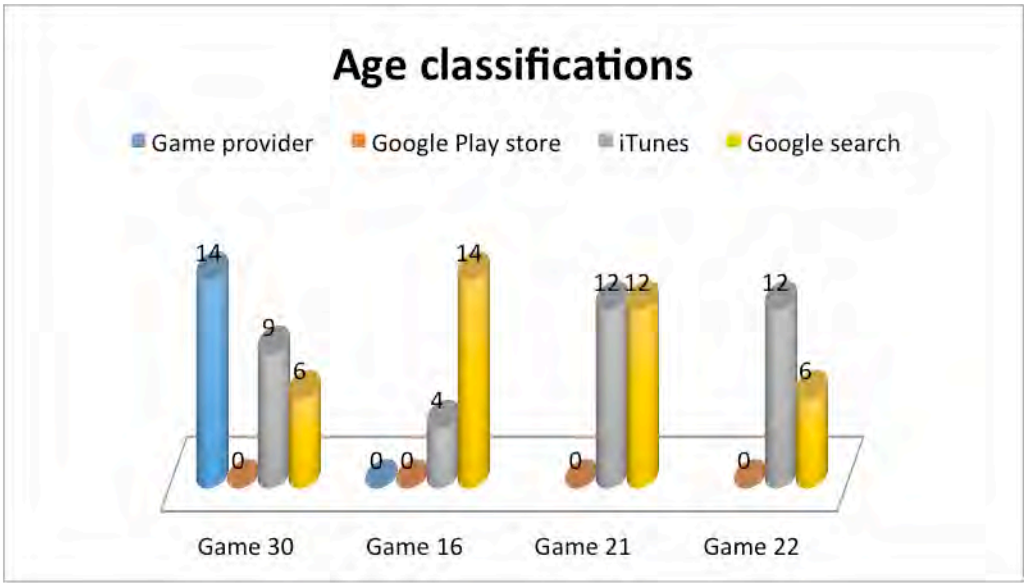

Diagram 2: Age classification by different sources

The tested online games were then compared by the source of age recommendation. The average age of the official source such as the USK in the German case, were compared to the average age recommendation classified by the individual game provider. In the cases of the online games game3 and game4, USK recommended age 6, while the game provider GC1 stated in their legal terms and condition that the recommend age is 18. Game4 was published from the same game provider and therefore also has the age recommendation of 18 years. But at the same time, the game provider published on the game's website the age recommendation of 12 years (see also diagram 3).

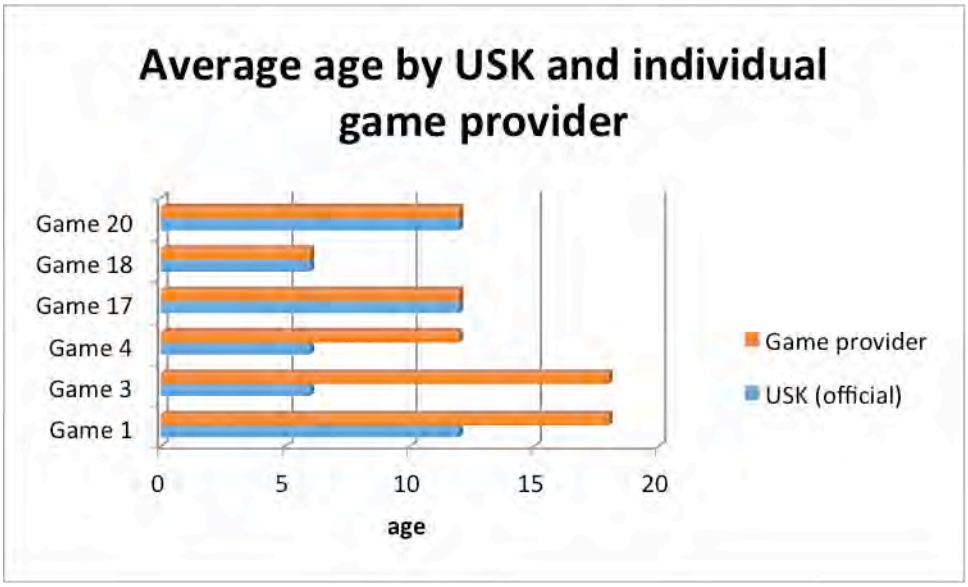

Diagram 3: Average age recommendation by USK and individual game provider

4.3 Analysis

The focus of age recommendation has taken a great part of this analysis. Age recommendation is the first step for parents to take in order to make sure that this specific game is applicable for their children and adolescents. Testing these online games has shown how difficult and unreliable age recommendation can be, and hence confuse or even mislead parents or other guardians, who try to act in their parental or guardian responsibility. Almost half of the here considered online games did not provide any age recommendations. Not only did the game provider fail to implement such important information but also official institutions such as the USK were not able to present age recommendation of the here chosen games. Noteworthy, the online games selected for this analysis were all well known and mainly published by German gaming companies. Additionally, age recommendations found, varied to such a great extend that reasonable conclusions by parents, guardians or children and adolescents could not be drawn. One interesting result presented by the data is the average age difference between the official site of USK and the game provider itself. Over half of the average age recommendations were not consistent, and thus inquiries need to be made whether the game providers should lower their age recommendation or USK should raise theirs. The latter seems more adequate considering the risks children and adolescents face in online games.

5 Payment Options

5.1 Background

After registering and downloading the adequate application for each online game, payment options were tested. Most of the online games contained tutorials, which provided insights of the games' interface and functionality. These tutorials were necessary to enable functions within the game while levelling up during the first steps provided in the tutorial. Functions enabled were for example access to wider geographical areas, a finding-friends-option and the chat functionality, which concerns the third issue considered in this paper. After finishing first tours and tutorials, payment fields could be clicked on in order to purchase virtual items such as coins, jewels, gems, elixir, weapons and thus upgrading ones character or kingdom. Payment options varied from game to game.

5.2 Methodological approach and results

Every game offered a minimum of eight different payment options or more. Even though, the focus of the payment method issue was to find out if they were any restrictions and in which way would they be available, the one most of interest was the telephone payment option. By clicking on the option "paying by telephone", two payment options were offered by the game. After choosing the desired item or amount, the user was asked to choose text messaging or dial a 0900- number.

All free-to-play online games inherited in-game purchase functions. Besides payment options such as debit card, credit card, transaction, PayPal and others (see Table Part 2, p.37f.), payment by phone was available in the majority of the tested games (see diagram 4).

Diagram 4: Number of games that offered payment options

Of all 32 tested games, no game had any further verification requirements in order to continue the payment procedure. The only restriction that was evident was the amount of money that could be spent during 0900 calls or text messaging. Some games only allowed amounts of the total sum of 10,00€ per call or text message. Noteworthy, some game provider advertised the simplicity of the purchase while purchasing a total amount of 49,99€, no registration was needed.

From all tested games only three online games did not provide telephone as a payment option. Twenty-nine of the tested games offered 0900 numbers to call or pay via text messaging (see also diagram 5). Noteworthy, the three games that did not offer payment option by phone are App games; purchases could only be made through in-App purchase. All other games provided the payment option paying via phone, e.g. payment through text messaging or fee-based hotlines. Other payment option that could be found were pay methods such as SponsorPay, which “rewards” the user with virtual items by signing up for online subscriptions.

Diagram 5: Number of games that offered payment option via phone

5.3 Analysis

Online game companies have changed the types of online games by offering free-to-play games in forms of browser or mobile games. At first glance, parents or children assume that the downloaded games are without further expenses. In-game purchases allow users to upgrade their characters, purchase virtual items such as coins, jewels, gems, weapons and other. Especially the payment option via phone was of interest in this analysis, but other payment methods should raise concerns. First of all, twenty-nine online games offered payments by telephone. Only a minority implemented restrictions such as a limited amount per phone call or text messages. However, the limitation of 10,00€ per call can easily be bypassed by calling anew the hotline such as the 0900 hotline[10]. This specific payment option does not face any "natural enemies" such as not possessing a credit card as a minor or facing a password lock in a mobile game. Children can easily access landline telephones as well as mobile phones, not being aware of high costs for purchasing magic coins. Another payment option that drew our attention was the payment method SponsorPay, which rewards the user with desired virtual currency by "only" clicking on subscriptions or surveys or other purchases. If children or adolescent play a free-to-play game on a family-owned mobile device such as an iPad, Apple-ID and thus the iTunes account is set up with an payment method, purchasing unintentionally online subscriptions, which will be done most likely as unaware as the high telephone bills produced during the cases described above. Consequently, the payment method SponsorPay needs to be equally of concern as the payment option by telephone.

6 Chat Function

6.1 Background

Additionally, the possibility of communication and interaction within the games were analysed. Similar steps as for analysing payment options were taken. After registration and first steps within the game, it was searched for chat functions and messaging possibilities. In some games, a great amount of time had to be spent due to limitations within the games. Limitations were for example the necessity to play and

[10] There is a possibility for parents and supervisors in Germany to block phone numbers such as 0900. Therefore, game providers do not consider themselves to bear liability. What makes this argument critical is the question of how many parents and supervisors have the knowledge of this payment option and the possibility to block it in the first place (Schulzki-Haddouti, 2014).

upgrade to a specific level before functions are enabled. Concluding into rather long involvement before amongst others chat functions were enabled. Other games provided chat functions from the start. Online games, which provided accessibility to other gamers only in higher levels, were consequently more time consuming to analyse. Chat options in the online games were called differently (guild chat, clan chat, global chat, buddy chat, etc.) but functionality was the same. The provision of opportunities to communicate with other gamers was usually shown in an open or global group chat. But other forms of communication and interaction between users were visible. Some online games also offered private communication possibilities between only two users. This could be similar to emailing or private messaging, without other players being able to follow up on messages and thus is considered more problematic when it comes to communication between adults and children.
The purpose of this analysis was to find out whether the game supplies chat channels, if yes, in which formats. Can any stranger contact anyone? Is there a private chat available, in which online perpetrators could gain a rather secure access to children?

6.2 Methodological approach and results

Twenty-six online games that were tested made communication channels for user to other users available. The forms of communication were different in each game, nevertheless, the overall chat function, which means adding and exchanging information with others was enabled by the game. Twenty-six games provided either one form or several forms of communication opportunities. Forms of communication that were found were global chat, private chat, guild and clan chat (see also diagram 6).

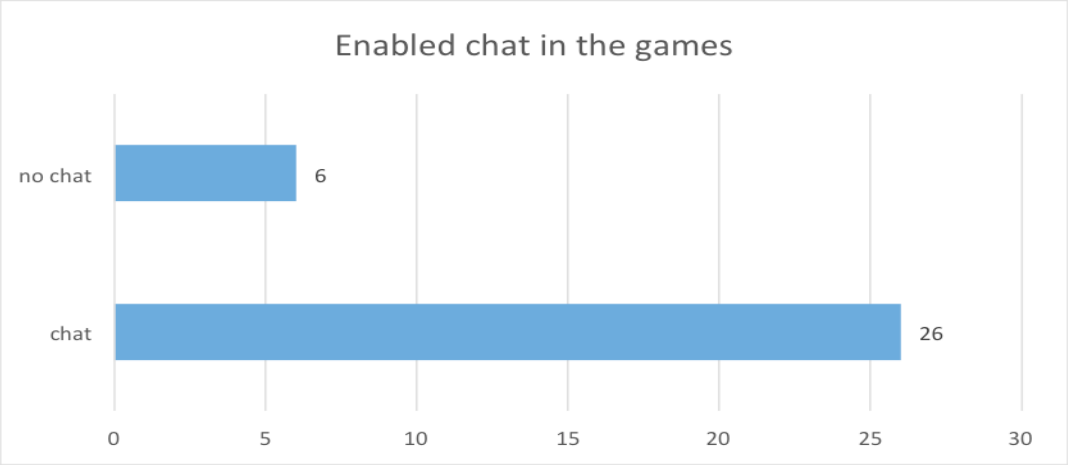

Diagram 6: Total amount of enablement of chat functions within online games

Only one of the tested games differentiated communication channels by the categories “buddies”; “alliances” and “strangers”.

6.3 Analysis

Nearly 81% of all tested online games grant strangers access to other gamers. Children and adolescents have many opportunities to communicate with other online gamers, not knowing whether the opponent is the person he or she claims to be. Twenty-six online games provide a global chat, a private chat or alliance-like chats such as clans and guilds. Related to the age issue, other gamers can claim any age, knowing that approximately 28% of 11 to 16 years old play online games in within European countries (EU kids online report, 2014). Furthermore, chats provide the opportunity to exchange personal information and thus privacy for children and adolescents can be endangered. This is especially questionable because a discussion about an ageless interaction and interplay of children and adults within an academic, economic or security discourse is (nearly) non-existent.

7 Conclusion

Risks factors considered in this analysis for children and adolescents were online sexual perpetration and financial losses as well as an inconsistent age recommendation. Moreover, other risks such as hate speech, cybermobbing and gamecrime are evident in online games. These risks are faced by children and adolescent in game environments and should not be underestimated and thus need recognition (Krebs & Rüdiger, 2010). As various studies show, online games are in many cases not (yet) considered as platforms that enable access to children and adolescents. Online Perpetrators can anonymously interact and communicate with children and adolescent without identifying themselves as adults. Online games create an increasingly entertaining and attractive virtual world in which children and adolescent enjoy being part of. Surprisingly then, that research regarding online games and the accessibility which online games provide between children and online perpetrator is nearly non-existent. Additionally, online games can vary in their types, F2P and P2P as well as on which device games are played. Only one study identified mobile gaming and thus app gaming as an increasing way of playing online games (getsafeonline, 2015). Still, this study did not include risks such as online perpetration and financial losses.

One consideration that should be more than problematic is the fact that in normal life, adults adapt their behaviour to children. For example, if a father plays football with his 6-year-old son, he will simply lighten his charges against the goal when his son is the goalkeeper. In order to do so, each game participant would need to know the (real) age of one another. None of the tested games or online games in general provides such an age labelling/marking/identification of the gamer. Hence, children and adolescents are exposed to risks considered in this paper, but also to risks such as bullying, pornography and extremism (Rüdiger & Pfeiffer, 2015; Rüdiger, 2016)

On the other hand, a visible age proclamation can also be counter-productive and thus, generating an even greater risk. Marking children as a child will make them more visible to online sexual perpetrators. Still, societal debates seem necessary in order to explain why we forbid games for children under the age of 18 in some cases, but allow adults to play and interact anonymously with children in other cases. Additionally, all tested games in this study were recommended either for the age 12 or under or age recommendation was unknown.

This is an issue that can only be addressed by society and an active process of negotiations in which the meaning of protecting children and youth in the virtual world has to be clarified and risk generators identified. The question that needs to be answered is: Should the Protection of Minors in the media (in German: Kinder- und Jugendmedienschutz) only inherit the task of stopping and preventing negative influences for children such as they do now by *recommending* and thus suggesting a certain age group for specific games? Or should they also be responsible for preventing crimes such as cyber grooming, sexual online perpetration and misused payment options and thus *restricting* certain age groups to access the game?

Considering all the risks, it is essential to understand that current research and legal regulations for online games and chat rooms still play “catch-up” with the rapidity of technological development such as MMORPGs and MMOGs provide. Therefore, considerations of widening responsibilities in order to protect children and adolescents accordingly can only be made when this particular issues are being identified and addressed.

Until now, game companies are insufficient regarding parental and guardian guiding as well as taking responsibility in order to protect children and adolescent from risks. As the research is scarce, so might be the knowledge of criminal activities in gaming environments. Even though, some research has focused on social media sites and

their chat rooms such as Facebook, MySpace and others, online games have scarcely been considered. In fact, except a blog entrance and the getsafeonline study cited earlier, online games seem to not play a significant role when considering online risks for children and adolescents.

By testing these 32 online games, it became clear, how strongly research in this area is needed in order to prevent crimes such as in the case of Breck Bednar.

References

Apple Support Forum: Warum kann ich nicht "Keine" auswählen, wenn ich die Zahlungsdaten meiner Apple-ID bearbeite? https://support.apple.com/de-de/HT203905. Retrieved: 1st of February 2016.

Ballard ME, Welch KM (2015) Virtual Warfare: Cyberbullying and Cyber-Victimization in MMOG Play. Games and Culture, 1-26.

Bundesverband Interaktiver Unterhaltungssoftware (BIU) (2014-1): Nutzerzah-len von Online-, Browser- oder App-Spielen http://www.biu-online.de/de/fakten/marktzahlen-1-halbjahr-2014/online-browser-und-app-spiele/nutzerzahlen-von-online-browser-oder-app-spielen.html, zuletzt geprüft am 03.02.2016

Cheong YG, Jensen AK, Guðnadóttir ER, Bae BC, Togelius J (2015) Detecting Predatory Behavior in Game Chats. IEEE TRANSACTIONS ON COMPUTATIONAL INTELLIGENCE AND AI IN GAMES, Vol. 7(3)3, 220-32.

Chuang YW (2015) Toward an Understanding of Uses and Gratifications Theory and the Sense of Virtual Community on Knowledge Sharing in Online Game Communities. International Journal of Information and Education Technology, Vol. 5(6), 472-76.

Cutlack G (2013) This Kid Blew $2,500 on In-Game Purchases in Just 10 Minutes. Gizmodo Uk. http://gizmodo.com/5987799/this-kid-blew-2500-on-in-game-purchases-in-just-10-minutes. Retrieved: 29th January 2016.

DateDoktor (2010) Achtung bei smeet.com! Forum___Hilferuf.de. http://www.hilferuf.de/forum/sonstiges/63803-smeet-de-2.html. Retrieved: 14th of February 2016

DeWalt KM, DeWalt BR (2011) Participant observation: a guide for fieldworkers. New York: AltaMira Press.

Diaz J (2015) Supercell Makes $5 Million Per Day off Clash of Clans. Androidheadlines. http://www.androidheadlines.com/2015/05/supercell-makes-5-million-per-day-off-clash-clans.html. Retrieved: 14th of February 2016.

Dirry, V / Rüdiger, TG (2015): Extremismus in digitalen Spielen. In: TG Rüdiger und A Pfeiffer (Hg.): Game! Crime? Frankfurt am Main: Verlag für Polizeiwissenschaft, S. 223–248.

Ducheneaut N, Yee N, Nickell E, Moore RJ (2006) "Alone Together?" Exploring the Social Dynamics of Massively Multiplayer Online Games. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 407-416.

Elgot J (2016) Breck Bednar's mother says killer has blogged from prison. The Guardian. http://www.theguardian.com/uk-news/2016/jan/27/breck-bednars-mother-says-his-killer-has-been-writing-blogs-online-from-prison. Retrieved: 14th of February 2016.

Emmison M (2004) The conceptualization and analysis of visual data, in D. Silverman (ed.) Qualitative Research: Theory, Methods, and Practice. London: Sage.

Evans M (2014) Breck Bednar murder: computer engineer admits killing oil millionaire's son. The Telegraph. http://www.telegraph.co.uk/news/uknews/crime/11252415/Breck-Bednar-murder-computer-engineer-admits-killing-oil-millionaires-son.html. Rerieved: 23rd of January 2016.

Foster H (1996) The Artist as Ethnographer. In: The Return of the Real. Cambridge, Mass. und London: MIT Press: 171–203.

Getsafeonline (2015) A third of parents feel out of control of kids' online gaming. https://www.getsafeonline.org/press/a-third-of-parents-feel-out-of-control-of-kids-online-gaming/. Retrieved: 21st of February 2016.

Hine C (2005): Virtual methods and the sociology of cyber-social-scientific knowledge In: Hine, Christine (Ed.): Virtual Methods. Issues in Social Research on the Internet, New York, 1-20.

Hollweck T (2014) Telekom storniert Handyrechnung von 4.700 Euro mit Posten von Google Play Store und BOKU Network. http://www.kanzlei-hollweck.de/2014/07/20/telekom-storniert-handyrechnung-von-4-700-euro-mit-posten-von-google-play-store-und-boku-network/. Retrieved: 17th of January 2016.

JIM- Studie (2015) Jugend, Information, (Multi-) Media- Basisstudie zum Medienumgang 12- bis 19- Jähriger in Deutschland. Stuttgart: Medienpädagogischer Forschungsverbund Südwest- mpfs.

Joint A (2003) Online Chatroom Regulation - Protecting children from paedophiles on the Internet. Computer Law & Security Report Vol. 19 (1), 44- 48.

Kempf, Dieter (2014): Studie "Kinder- und Jugend 3.0". Online verfügbar unter http://www.bitkom.org/files/documents/BITKOM_Publikation_Netzgesellschaft.pdf, zuletzt geprüft am 06.09.2015

Kierkegaard S (2008) Online child protection Cybering, online grooming and age-play. Computer Law & Security Report 24, 41–55.

Krebs C, Rüdiger, TG (2010): Gamecrime und Metacrime. Strafrechtlich relevante Handlungen im Zusammenhang mit virtuellen Wel-ten. Frankfurt, M.: Verl. für Polizeiwiss.

Livingstone S, Haddon L (2014) EU kids online. Findings, methods and recommendations. EU kids online report 2014. https://lsedesignunit.com/EUKidsOnline/index.html?r=64. Retrieved: 29th of January 2016.

Lipka M (2014) Apple Offers Parents Refunds For In-App Purchases By Kids. Huffington Post. http://www.huffingtonpost.com/2014/03/31/apple-offers-parents-refunds-for-app-purchases_n_5062844.html. Retrieved: 14th of February 2016.

Mann C & Stewart F (2000) Internet Communication and Qualitative Research: A Handbook for Researching Online. London: Sage.

Markham A (2004) Internet Communication as a tool for Qualitative Research, in D. Silverman (ed.) Qualitative Research: Theory, Methods, and Practice. London: Sage.

Martinson J (2013) Apple's in-app game charges: how my kids ran up huge bills.

http://www.theguardian.com/technology/shortcuts/2013/mar/26/apples-in-app-game-charges-kids-bills. Retrieved: 22nd of January 2016.

Moore A (2016) I couldn't save my child from being killed by an online predator. The Guardian. http://www.theguardian.com/lifeandstyle/2016/jan/23/breck-bednar-murder-online-grooming-gaming-lorin-lafave. Retrieved: 23rd of January 2016.

Moser C (2014) BOY SPENDS OVER $46,000 IN FREE-TO-PLAY GAME. http://www.ign.com/articles/2014/10/03/boy-spends-over-46000-in-free-to-play-game. Retrieved: 28th of January 2016.

Narcisse E (2014) 15-Year-Old Kid Spends 37,000 Euros on Gold in Free-to-Play Game. http://kotaku.com/15-year-old-kid-spends-37-000-euros-on-gold-in-free-to-1642091831. Retrieved: 31st of January 2016.

Online games. http://www.pegionline.eu/en/index/id/233. Retrieved: 27th of Janauary 2016.

Rüdiger TG (2015a) The Real World of Sexual Predators and Online Gaming. Blog-Beitrag BeAKidsHero. http://www.beakidshero.com/posts/the-real-world-of-sexual-predators-and-online-gaming/. Retrieved: 18th of January 2016.

Rüdiger, TG (2015b): Der böse Onkel im virtuellen Schlaraffen-land - Wie Sexualtäter Onlinegames nutzen. In: Thomas-Gabriel Rüdiger und Alexander Pfeiffer (Hg.): Game! Crime? Frankfurt am Main: Verlag für Polizeiwissenschaft, S. 142–159.

Rüdiger TG; Pfeiffer A (Hg.) (2015): Game! Crime? Frankfurt am Main: Verlag für Polizeiwissenschaft.

Rüdiger, TG (2016): Onlinespiele - Ein kritisches Spielfeld für Kinder und Erwachsene? Eine kriminologische Betrachtung auf das alterslose Zusammenspiel in Onlinespielen. In: Junge,Thorsten/Clausen, Dennis (Hrsg.): Digitale Spiele im Diskurs.

Sauerbrey A (2015) Cybergroomer: Missbrauch im Internet - Falsche Freunde im Netz. Der Tagesspiegel.
http://www.tagesspiegel.de/weltspiegel/sonntag/cybergroomer-missbrauch-im-internet-falsche-freunde-im-netz/12249066.html. Retrieved: 14th of February 2016.

Scheerhout J (2016) Paedophiles using Clash of Clans and Instagram to groom

children as young as seven. Mirror UK. http://www.mirror.co.uk/news/uk-news/paedophiles-using-clash-clans-instagram-7117707#ICID=sharebar_facebook. Retrieved: 14th of February 2016.

Schulzki-Haddouti C (2014) Chats in Online-Spielen bleiben unberücksichtigt. Golem. http://www.golem.de/news/jugendschutzvertrag-und-usk-chats-in-online-spielen-bleiben-unberuecksichtigt-1403-105420.html. Retrieved: 22nd of February 2016.

Second life. http://secondlife.com. Retrieved: 3rd of February 2016.

Sevriens D (2011) Die Berufung der Klägerin gegen das am 26.02.2010 verkündete Urteil des Amtsgerichts Saarbrücken (Az.37 C 312/09(02)) wird zurückgewiesen. http://www.wmwllp.de/berlinblawg/urteile/verbraucherrecht/lg-saarbruecken-10-s-60-10/. Retrieved: 22nd of February.

Spradley JP (1980) Participant observation. United States of America: Holt, Rinehart and Winston.

Statista (2015a). http://www.statista.com/statistics/271930/time-children-spend-playing-mobile-games/. Retrieved: 22nd of February.

Statista (2015b) http://www.statista.com/statistics/270291/popular-categories-in-the-app-store/. Retrieved: 22nd of February.

Supercell. Terms of service. http://supercell.com/en/terms-of-service/. Retrieved: 1th of February 2016.

Svahn C (2015) Gratisspel kostade familjen 60.000 kronor. Dagens Nyheter. http://www.dn.se/ekonomi/gratisspel-kostade-familjen-60000-kronor/. Retrieved: 12th of September 2015.

Temmerman M (2014) 37.000-euro van mama verspeeld met 'gratis' game. http://www.nieuwsblad.be/cnt/dmf20141002_01300598. Retrieved: 31st of January 2016.

Wallop H (2014) My son spent hundreds of pounds on in-app purchases without me knowing. The telegraph. http://www.telegraph.co.uk/men/relationships/fatherhood/10886939/My-son-spent-

hundreds-of-pounds-on-in-app-purchases-without-me-knowing.html. Retrieved: 29th of January 2016.

Williams D & Skoric M (2005) Internet Fantasy Violence: A Test of Aggression in an Online Game. Communication Monographs Vol. 72 (2): 217–233.

Williams M (2007) Avatar watching: participant observation in graphical online environments. Qualitative Research Vol. 7(5): 5-24.

Webopedia. In-App purchases. http://www.webopedia.com/TERM/I/in-app_purchase.html. Retrieved: 3rd of February 2016.

About the authors

Diana Selck is a German criminologist student at the University of Hamburg. Her focus in criminological research is in crime and aggressive behaviour online. She is mostly interested in interpersonal relationships that develop through communication and interaction on online platforms and establish opportunities to meet strangers whom take on identities, which do not correspondent to their real selves. The focus of her current research project is to analyse victimisation processes through online romance scam and webcam blackmail. Both of these online crimes correlate with research in scam and fraud, online grooming, dating scam and sextortion. In 2015, she began managing a Facebook page called *researching cyberaggressions – online romance scam, sextortion*, which aims to inform and educate individuals about new forms of online crimes such as webcam blackmail (often called sextortion), online romance scam and other aggressive behaviour online. Connect with Diana on Twitter.

Contact: diana.selck@googlemail.com

Thomas-Gabriel Rüdiger is a German criminologist, researcher and lecturer at the Institute for Police Science at the University of Applied Science of the Brandenburg Police. He is an expert in criminological research regarding digital policing – especially the usage of social media for digital community policing; the development of norms as well as their judicial review in digital space and its online crimes. His focus is with emphasis on youth violence and sexual delinquency, hatespeech, cyber crime, and risks in web social communities and virtual worlds (in particular, online gaming). In this particular space, he consults political and juridical instances as well as NGOs and is often asked for interviews focusing on digital risks and regulation and control possibilities in leading German media. In 2013, Thomas-Gabriel was awarded the first European Future Award for Policework for his publication "*Gamecrime*" about crime in virtual worlds. Connect with Thomas-Gabriel on Twitter.

Contact: thomas.ruediger@fhpolbb.de