32

Actual Policing in Virtual Reality – A Cause of Moral Panic or a Justified Need?

Katalin Parti
National Institute of Criminology,
Hungary

1. Introduction

This study aims to describe those aspects that qualify a form of behaviour as a crime in the virtual communities, these highly organised societies of the Internet. But the image of deviances may not be complete without entities watching over them. It is an interesting question, who could lay down and enforce virtual norms, if not the community itself. Today, organised crime, drug trafficking, money laundering, trafficking in human beings, and sexual exploitation of children are such focal issues of criminal law, whose prosecution does not stop at the boundaries of virtual communities, or the Internet. But what justification does the real world's jurisdiction have to intervene in the everyday life of independent virtual communities? If they have the right, who decides on the involvement of real authorities? What legal regulations does real-life law enforcement apply in a virtual space? Is there an appropriate response to crimes committed in the virtual world by real-life jurisdiction, and can different forms of virtual deviance be prevented with the tools of real-life crime prevention? These are the questions that I wish to answer in the followings.

2. Types of virtual communities

There are several attempts at classifying *online* communities. Williams believes that online communities are defined by technical development.[1] (Williams, 2010) The first phase of development is web 1.0, where users communicate with each other using electronic mailing systems, newsgroups and instant messages (e.g. MSN messenger). These platforms are static websites whose aim is forwarding textual information. Web 2.0 technology goes a little further than that, involves real-time interpersonal interaction and web content generation appears. Users may edit the contents of a webpage themselves. The more content there is, the greater the demand for the democratisation of content (e.g. wikis, blogs, social networking sites such as Facebook, MySpace, eBay, Bebo). The next step, web 3.0 technology is just taking shape today. This technology makes online interactivity more realistic, life-like and direct with its 3D graphic surfaces (e.g. Second Life, Habbo Hotel, Active Worlds). Users may enter these online surfaces represented by their virtual alteregos, the avatars. Most of these worlds allow their users several activities mimicking reality, such as for

[1] "*Web is increasingly socialized*" - notes Williams.

example buying a real estate or building a house in the virtual space, and having virtual movables. (Williams, 2010)

Reynolds classifies today's virtual realities as follows (*Four World Theory*). There are online realities whose essence lies in playing together (ludic worlds), based on the rules set by the maker of the game. These communities can not change their rules, and those who do not like the given world may leave (e.g. World of Warcraft). But 'games' in a less traditional sense have also appeared. These communities copy the social order of the real world (social or civic worlds; e.g. Habbo Hotel, Second Life). The rules in these virtual worlds are laid down by the operator of the platform, but the users may have a much greater influence on the rules of civic worlds, and therefore they have more independence. Civic worlds are the closest copies of the geographical world. (Reynolds, 2005)

Groups of people, who not only support their current offline lives with new technological developments, but go a step further, and use thechnology to create and live a new life, are called virtual realities (VR) in Williams' theory. (Williams, 2006) VR is a graphically developed, virtual online social space created in a 3D environment.

In my interpretation, all users of the Internet are part of some online community. These may be e-mailing communities, but also websites, forums, chatrooms and online games or virtual communities modelled on reality (social or civic communities). Online communities, just as offline (geographical) communities are held together by shared interests, sociability, dialogue and the continuity and regularity of joint action. All Internet users belong to one or another community at their level, and all users of the Internet have the opportunity to overstep the limits of communities of various organisational levels, and join new communities. (For instance, users of Second Life[2] regularly keep contact with each other and other communities on other platforms – forums, chatrooms, websites and e-mails. Boellstorff, 2008)

In the following, I wish to discuss those online forms of deviance that occur in highly organised **civic** and **social worlds.** These well-developed online communities are modelled on reality, both in their technical realisation (3D visualisation), and objectives (making contact, the experience of being part of a community, and the recreation of the rules of traditional community life). I will attempt to describe the forms of deviance, the reasons of crime, the nature of harm, and the legality and effectiveness of the intervention of geographic jurisdiction.

3. Where does virtual harm begin?

3.1 The concept of harm in virtual worlds

Williams classifies harms occuring in online communities. (Williams, 2006) According to him, there are **1. cybercrimes, 2. cyber deviances, and 3. cyber harms.** While a cybercrime is a black letter crime procesuted by geographical criminal law and authorities, cyber deviances and cyber harms are harms caused in VR. Cyber harm is an activity which damages or offends one particular member of the community, but does not obviously violate everybody's idea of morals in general. In contrast, cyber deviance is a harmful act which the whole or the majority of the community but at least its leading personalities

[2] Second Life invented and created by Linden Laboratory Inc. California is a 3D social/civic space on the Internet. As its name implies, it is a virtual world in which members create an avatar and then use that character to live out a separate existence.

consider to be subversive for the community and as such, intolerable. We can also see that acts of one category sometimes turn into another. In relation to the spread of all annoying acts, it is more common for cyber harms to turn into deviances, and deviances into cybercrimes, than the other way round. The case of online harassment is a good example. Offline legal regulations already foresee punishment for the online forms of hate speech. Or let us take ageplay, the sexual exploitation of children[3] in the virtual world which used to be an isolated phenomenon with fews cases, but these days acts committed in VR are prosecuted in line with geographical legal regulations. These responses are justified by political, legal and social pressure, when the state is of the opinion that they have to do something against the situation considered to be 'unbearable' by certain interest groups. More 'esoteric' (not tangible, less clearly outlined) and less grave acts are left to the judgement of online communities. (Williams, 2006) These are the acts that later turn into offline criminal acts, which are grave enough to go beyond the limitations of response of online communites. (Williams, 2006)

The problem is that in many cases it is impossible to decide, whether cyber harm and cyber deviance qualify as cybercrime, and as such whether it is subject to the state's obligation to enforce criminal law, for the protection of its citizens. To give you a better idea of the confusion, let us see first what kind of deviances may occur in VR and what sets them apart from geographical crimes.

There have been many and varied attempts to classify cyber deviances. (See for instance Williams, 2006; 2010; Wykes, 2010) One of the better known classifications is given by Wall. (Wall, 2001) According to him, the first group is **cyber trespass** (information warfare: invasion of private space on the Internet by a hacker causing data loss and possibly economic standstill). The second group is **cyber theft** (spoofing, phishing, pharming, identity theft, cyber copyright infringement), where the user poses as an avatar of someone else which is achieved by hacking a user's account. (Williams, 2010) The third group is **cyber obscenity** (legal pornography and sexual misuse of children). (Rimm, 1995; Mehta & Plaza, 1997; Harmon & Boeringer, 1997) The fourth group is **cyber violence** (manifests in textual, visual and audio forms) which can be further divided as follows.

1. Flaming: debates on message boards and e-mails, containing text messages about others to a humiliating and libeleous effect. (Joinson, 2003)
2. Hate speech digital performances: digital performances inciting hatred, e.g. racist, homophobic or extremist websites. (Mann et al., 2003)
3. Online stalking: harassment through computer mediated communication (CMC) for the purpose of gaining information, intimidation, or simply contact with a non-consenting person. (Reno, 1999; Bocij, 2004; Meloy, 1998)
4. Virtual rape: while the stalker only sends messages, the virtual rapist brings the victim to act against his or her will.[4] (MacKinnon, 1997; Reid, 1999; Dibbel, 1998)

In my interpretation, there are **two underlying deviances in the virtual world**, depending on whether the actual (psychological or physical) damage is to the affected person or the

[3] The politically correct name of the phenomenon known from the media as 'child pornography'is 'child sexual abuse'. 'Pornography' assumes that the parties involved are equal, while a contact of sexual nature with a child is always abuse.

[4] One form of virtual rape is when the offender animates avatars against the wishes of their owners, and controls them to do humiliating things, e.g. entering a sexual relationship with another avatar against their will.

property created/represented by him/her. In that sense, slander, defamation, contribution to suicide, bodily harm, manslaughter, or crimes against sexual morals, among others, are forms of deviance against persons. Deviances against property are mainly causing financial damage, e.g. theft, copying without permission, damaging and destruction of objects created by avatars. Vandalism can belong to any of the two, depending on the nature of the damage caused.

3.1.1 Deviances against the person in virtual worlds

Judging **virtual deviances against persons** on the basis of geographical law is complicated, since the 'person' is missing, and the user is only present and contacting others in VR through his/her virtual alterego, but not in person. (Wall bases his opposites, cybercrime and meatcrime, on the same logic. Wall, 2010) For this reason, we could possibly treat crimes in the virtual world as attempts perpetrated on an unsuitable subject or with an unsuitable instrument. Practice, however, shows that this approach is misleading.

Deviances against persons are particularly dangerous, because the individual may sustain serious **psychological scars** even during textual communication. In the virtual world, textual communication is the substitute of verbal self-expression. Communication plays a role in identifying a person's place in social hierarchy. Hate speech can be especially destructive. (Becker et al., 2000; Matsuda et al., 1993; Butler, 1997) Hate speech, slander and defamation appear in online communities both as illocutionary and perlocutionary acts. (Austin, 1975) It is possible that a verbal (textual) insult only achieves its effect, when the addressee reads it. This may be immediate – typically in 3D social/civic community spaces – , or delayed, – e.g. when the addressee opens the message sent in an e-mail or posted on a message board. In CMC, real time conversation means that the addressee receives the message immediately, at the same time as it was written, which has an immediate effect. This is characteristic of most interactions in online communities. The text is however supplemented with emoticons, and phatic communication (e.g. using capitals for shouting). Because online communication is so expressive, it is no coincidence, that terrestrial law has conquered the online world with a ban on hate speech. The reason for this is that online texts may cause greater damage than spoken words. Online texts are written, can be re-read, and therefore get more deeply imprinted on the mind of the victim, moreover they invariably leave a trace on the Internet. At the same time, it is possible that the defamatory message is read by others which may unstabilise the individual's position and reputation in the community. (Markham, 1998; Turkle, 1995; MacKinnon, 1997) The offensive remarks put the opportunity of change and the control into the hands of the offender, who becomes a person of authority. (Delgado, 1993)

3.1.2 Deviances against property (of financial nature) in virtual worlds

Users may not only suffer psychological, but also actual **financial damage** in virtual worlds. Residents of virtual communities are often looking for opportunities to create themselves. (Oldenburg, 1999, quoted by Williams, 2006) In the virtual space, residents are free to create. They may pursue any creative, and at the same time lucrative business activity, like building houses, writing scripts for furniture, other pieces of home equipment and decorations, and for the appearance of avatars (scripting, fashion designing, motion design for avatars). Just like in the geographical world, residents of virtual communities can live on their takings from services sold. (Boellstorff, 2008) As residents may also trade their goods and services, the creation of goods is not merely a channel for self-expression, but also a job, as it represents financial value. Residents have no limitations in 'building', there is no central power that would limit creative self-expression for political or economic reasons. Virtual space is therefore also called **creationist capitalism**, where work is not compulsory, but a leasure activity, or even the primary form of self expression. This is why Boellstorff calls the internal structure of online communities playful capitalism, or ludocapitalism, where "production is melting into play". (Boellstorff, 2008: 206) Hence, in virtual worlds, the development of skills corresponds to the production of goods. This was the ideology that lead the creators of several virtual spaces to enable users to convert their income from virtual goods into an offline currency.[5] The creationist capitalism aspect of virtual worlds is further strengthened by the migration of business activities into the realm of the Internet. This is what Yar calls informational economy. (Yar, 2010, referring post-industrial capitalism at Bell, 1999, and Castells, 2002)

As we can see, virtual space is a free space which enables users to express themselves while generating financial profit. The larger the profit generated, the higher the risk of the creator. Financial gain gives a basis to possibly damaging actions. It is therefore indubitable that one may suffer damage in the virtual space, just as in the real world, through the loss, damage or destruction of goods created.

3.1.3 Cyber vandalism

The above classification should be completed with **cyber vandalism which neither fits into the category of deviances purely against property, nor those purely against persons**. Virtual vandalism means that the offender damages or destroys objects created and/or possessed by avatars, but this may cause psychological damage as well. When virtual objects are vandalised, they are not destroyed for good, as the scripts and codes can be restored, but there is damage done, of a material or psychological nature, if objects of sentimental value, such as gravestones, religious artefacts, devotional articles, or souvenirs are destroyed. (Williams, 2004)

In VR, constructions are a symbol of affiliation, as the act of building is also a symbol of belonging to the community. The vandalisation of institutions symbolising the community (buildings, memorial sites or tablets) is a means of renouncing community existance and breaking down community cohesion. (Williams, 2010) The more such attacks there are, the more fragmented the community becomes, as people are less happy to participate in community activities if the symbols of belonging are regularly vandalised. (For 'avoidance behaviour' of community members see Williams, 2006: 81, 83) If the community is weakened, online friendships will also weaken, and these are the essence of an online community. If we accept that online friendships are just as important as offline ones, then any harm done to online friendships may be just as painful a loss as losing a friend or the entire community in the offline world. Similarly, if a formal police building is created in the online world, it reassures the community, can be a means of prevention, and also strengthens ties to the community.

The umbrella term for the different forms of cyber vandalism that is **virtual violence against persons and objects** – or put simply 'causing disturbance to others' – is **griefing.**

[5] Sims Online was the first virtual space based on creationist capitalism. In 2004, 99% of objects were created by residents. (Ondrejka, 2004) Inspired by that, Second Life, launched in 2003, follows the strategy of a user-created inworld exclusively.

(Boellstorff, 2008; Williams, 2010) This may be a criminal or sub-criminal act, that is a crime or a deviance. For example, sending unsolicited e-mails with obscene, intimidating, or abusive content, or the publication of the personal data of an individual on a message board (data theft), which may lead to unsolicited contact, or libel and defamation (personal harm). But it may also involve the commission of deviant activities under the name of the assumed personality, and pretended friendships and business relations.[6] **Boellstorff believes that griefing** is 1. an intentional action 2. which is aimed at disturbing others, 3. that the griefer enjoys. (Boellstorff, 2008; Foo, 2004; Mulligan & Patrovsky, 2003) This stems in the fact that in online communities people are freed of their inhibitions (disinhibition). A positive manifestation of this is when people are altruistic, kind, and a negative one if "people think they can shoot and run", they can not be identified anyway. Anonymity makes offenders unscrupulous, and this also helps them to keep the victim depersonalised, and neutralise their deeds. (Curtis, 1992) Griefing never harms the victim in his actual physical form, it is therefore less frightening, less grave than its offline counterpart. The harasser and the harassed do not meet in person, and in most cases the harassment is in written form, and not in person. Other senses are not involved (such as smell, touch, vision and hearing). (Williams, 2010) So people can not be harmed physically by greifing, but on the other hand, it may cause serious financial damage, if for example griefing is used in business activities.

3.2 Contact points of virtual and geographical deviances

As we see, the concept of harm is somewhat different from the usual norms of the geographical world. In the VR, the concept of damage and harm is to be viewed in an abstract sense. There is for example no damage done if a suicide bomber blows himself up, as it does not endanger the lives of other avatars. It is another question that the users created the objects destroyed or damaged in such an attack with actual financial investments, and therefore there may be material damage. The users themselves behind the avatars, however, do not suffer any personal damage.

According to some research, cyber deviances do not always remain within the realm of online worlds, but can **migrate** to offline environments. (Quayle, 2010; Williams, 2006) A real world manifestation of griefing may be offline bullying, or teasing. (Schechner, 1988) Online stalking may give rise to offline stalking. John Robinson, who became known in the online community Cyberworld as Slavemaster was arrested in June 2000 by Kansas State police. He had several victims offline. The last of them was Susette Trouten, a member on Cyberworlds. Both of them participated in sado-masochistic rituals in the online community. Suzette also met the offender, who later killed him, offline. (ABCNews.com, 2000) Cyberworlds created a whole philosophy and phantasy world around sado-maso games, whose believers also realised their acts offline. Suzette Trouten fell victim to these. Reno believes that online stalking can be especially dangerous, as it may be a prelude to its physical manifestation. (Reno, 1999)

[6] Boellstorff presents a whole array of griefing. The amassing of junk in the online community space is a form of griefing, just like placing provocative objects (e.g. giant dildos) in central community spaces, but the mobbing of an avatar and talking to him abusively, or sending abusive, threatening, or intimidating instant messages to several residents are also forms of mobbing. It is particularly disturbing if the avatars are animated against the wishes of their owners, and are made to perform humiliating things. (Boellstorff, 2008)

According to research, it is not advisable to play down virtual harms. In 3D virtual communities **stronger bonds** may develop **than in earlier online communities** only based on textual communication (message boards, bulletin boards, etc.) as the virtual representation of the self appears here, which, together with emote commands deepens feelings and interactivity. (Bocij, 2004) Other research go even further than that, and claim that in the virtual world, **stronger community bonds than in the geographical world** may develop. In real life, we are constantly busy working and taking care of other important things, and we are performance oriented. As opposed to that, in the virtual world, we are more free, have more time, also to pay attention to others, as we are spending our leasure time at the online community. This makes people in the VR more open, more accepting, friendly, and even altruistic. (Boellstorff, 2008) An alternative social arena serves the very purpose of preventing and replacing the dysfunctional social relationships in the offline world. (Oldenburg, 1999) The bond has a significance in defining the **degree of harm**. The stronger the bond to the community, the greater the harm suffered.

We saw now that **virtual and actual are not clearly separated**. Either because online deeds may lead to offline ones, or because the online acts may cause actual psychological or financial damage in the real world. But it is impossible to establish the extent of the harm done in a virtual world. One of the reasons for this is that geographical harm-conception is not taken over one-to-one and also due to statistical problems.

4. Legislative trend – a shift to the virtual

4.1 The actors of moral panic

There are **no reliable statistics** for virtual crimes due to their complexity and their judgement varying from country to country. There are records available, but these mainly contain data collected primarily for financial and less for criminal law reasons, their data fields are not always compatible which makes comparisons impossible. (Wall, 2001) Damage suffered in an online environment very often does not materialise, and if there is material damage, it is very difficult to assess. (Wall, 2008; Moitra, 2003)

There may be no reporting if the victims are not aware of the attack, (Murff, 2007; Moitra, 2003) or perhaps the given country is not yet prepared for registering attacks carried out in computer systems, or the given act is not punishable under applicable law, or there is no forum (administrator or VR community arbitration) where the victim could report to. It is also possible that the victim has reported an offence, but the party entitled to judge the complaint believes there is no need for further measures in the case. Cybercrimes are defined in different ways in the criminal codes of different countries, even though the Council of Europe and the European Union made considerable efforts to unify legislation for laying the foundations of international criminal cooperation and the more effective prosecution of crimes.[7] The development of technology, however, is far more progressing than legislation, so acts may occur which have not been defined properly by law. (Lacey, 2002) Such is for example harassment in a virtual environment which according to

[7] The Council of Europe's treaty on cybercrimes adopted in Budapest on November 23, 2001 can be regarded as the first significant global unification agreement. (Convention on Cybercime, CETS. No. 185 – 23.XI.2001.) At European Union level, Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography is the most significant effort. (OJ L 13/44-8)

geographical law, is not obviously classified as a crime. (Online harassment is very often only meant to disturb, and does not always contain an intimidation element. Geographical law, however, almost always demands an emotional effect for the act to qualify as harassment. See Bocij, 2004) The fact that there is no exact statistical data on the volume of deviances occurring in virtual spaces, only further increases the panic, as it may give the impression that virtual deviances are not transparent and uncontrollable. (Wall, 2008)

Overemphasising the negative effects of the Internet and its virtual communities is basically generating moral panic. This is where the responsibility of **traditional media** shows (I refer to the press, radio, and television as traditional media, offering pre-filtered contents to the audiences). Traditional media are true catalyst of moral panic, because by the very principles of their operation, it enhances the panic effect. Only shocking, scandalous or scary information has any newsworthiness. These media present such information in a pre-filtered manner, lifted out of the original context. Programmes that expressly emphasise the *fact* of downfall of morals, of the crisis of values and of the moral crisis further add to this. (Parti, 2010)

However, not only media news trigger panic. **Scientific research** on changes of behaviour in relation to the new medium, the Internet, can also fuel moral panic. Science may be objective in its principles, but it still can not explain a lot of phenomena, or predict their effects (see e.g. what an effect the presence in a VR community may have on the personality), and in such cases resorts to guesswork when looking for arguments and consequences.

Aversions towards cyber-communities are born out of the threat of emerging cyber-deviances. A cyber-deviance in general means the adjustment to the online environment coupled with double moral standards. Double moral standard (Michelet, 2003) means that the majority of users traditionally respects accepted norms, but in VR communities they live by different standards (e.g. they would not steal a mobile phone or a bag, but they have no qualms about downloading copyrighted software which is also illegal). These double moral standards are nourished by people's faith in anonymity that is the belief that the parties communicating online are unidentifiable.

Some social scientists even claim that the spread of online communication leads to the complete decline of existing moral values. The reason for this is the mass appearance of harmful contents on the Internet and their availability to anyone, especially youngsters. Such contents – like pornography, xenophobia, incitement to hatred or extremist ideas – were not available to anyone before the Internet age and were very difficult to spread. As by now everybody can potentially access these materials, they are becoming increasingly extreme due to the competition.

Moral panic is not only society's spontaneous reaction to the spread of a disturbing activity (deviance) or a new phenomenon. Such are for example today's moral panic reactions to the Internet as new technology, and the media. Some believe that causing panic is a means of governments in general to manage new, earlier unknown social symptoms. Panic can therefore also be an artificially generated balancing power, and as such, a means of prevention. (Parti, 2009) Moral panic, whatever triggers it, is suitable for repeatedly developing people's self-control.

Causing panic at government level can be justified less with the publication of perceived or actual facts or suppositions, than with intentions of prevention. Frank Füredi in his book on risk society (Füredi, 1997) elaborates that in a 'culture of fear' our interpersonal relations become dangerous. Above all, we have to concentrate on maintaining our private sphere, as that is the most likely to be affected. Füredi says that hysterisation keeps appearing in new areas.[8] This is, however, primarily not related to the dissemination of knowledge and information, but prevention. For example, The US government did not tell the truth, when they labelled AIDS as the greatest risk of homosexuals. (Füredi, 1997) Looking back, however, society tolerates this 'benign lie', because the government could only move people to practice self-moderation and self-control with this exaggerated prevention campaign. With this purpose in mind, it is not so obvious anymore whether in a similar situation we should tell the truth, or make use of a white lie as a means of prevention. According to another branch of the consciously caused panic theory which in many respects is similar to panic triggered by the media, moral panic is a means to maintain political power. This is similar to panic caused by the media in that both use panic as a means to achieve their own goals. (Korinek, 2006)

Garland and Simon (Garland, 2001; Simon, 2007) believe that politicians and crime prevention policy makers use this panic for tactical purposes, for crime prevention and risk control. They use the same tactics for cybercrime which is not surprising at all. Taipale calls the fear of technology FrankenTech. (Taipale, 2006) The developers of technology are often involved in crime prevention policies (including activists and the media), and it is in their interest to exaggerate the threat of cybercrime, as it sells their products. The gap between the expected (perceived) threat and the security-measures corresponds to the gap lying between the numerous cybercrime cases reported by media and the few actually solved by law enforcement. This is a so called 'reassurance gap' that needs to be bridged. (Innes 2004) A typical example for the need for reassurance is the public's need for stricter and more detailed legal regulations and police action. This is obviously impossible to realise, because it is not only the supposedly large number of crime and their wide-spread nature that is missing, but also the police forces are more prepared for mass response to crimes already committed than prevention and monitoring of those in the grey zone. (Wall, 2007)

Legislation on the new medium – even though only indirectly – also contributes to the deepening of the moral panic. Legislation is always based on scientific research and consultation with experts, but it can not shake off the effect of politics either. **Political interests** always try to ensure that public opinion prevails, and are certainly under pressure from the public opinion. For this reason, legislation also can not remain completely unaffected by the moral trends triggered by the feeling of panic. (Parti, 2010)

Legislation trends in recent times point to the penalisation of an ever wider circle of acts, the criminalisation of preparatory acts, and the exaggerated regulation of details.

4.2 The reverberations of moral panic in legislation – through the example of child sexual abuse

Of all waves of panic, perhaps the most pervasive is related to the sexual exploitation of children. (Jenkins, 1998). A research of Carnegie Mellon Univesity (Rimm, 1995) found in the early 1990s, that about half of all Internet content is of pornographic nature. Even though since then, this research has been proven to be methodologically flawed, it is still regarded

[8] Such is for example the sincerety of romantic relationships – can we believe it will last?; the safety of single women – will men really protect them, or rather bring more danger?; genetic engineering – what effects do genetically modified foods have on our body and environment?; state-of-the-art technologies – is it safe to use air conditioners in the office, or on an airplane?; Internet communication – is it safe, or does it lead to the abuse of our data?

as the moral panic genesis of the Internet. The moral panic is, however, not entirely unfounded, as with the advent of the Internet the online sex industry started to develop explosively and still has a huge financial potential. (Wall, 2001; Casey, 2004) This created a never-before-seen competition situation online, so that the pornography industry is forced to make its products more extreme, just to maintain demand. This extremisation mainly shows in the increasingly lower age of the actors. (Parti, 2010) Another element of the pornography panic is that consumers may become immune or indifferent to traditional pornography. The usual contents are not enough for old consumers, they always want something new and more exciting. Also, Internet users not consuming pornography are involuntarily faced with it online with increasing regularity which leads to a gradual desensitisation towards extreme contents. The following table shows how the nature of pornography has developed as a cause of the rise of the Internet.

When?	The audience of pornography	General opinion on pornography	Social attitude
Before the Internet	Targeted groups: marketeers, black market, news agents, buyers of erotic literature, visitors of video rental shops	‘Extreme’	Excluding, rejecting
After the appearance and spread of the Internet	Groups are not specifically targeted: everybody with an Internet connection	‘Ordinary’	Tolerant, accepting

Table: The transformation of pornography with the appearance of the Internet (Parti, 2010)

Panic also shows in legislation. The most recent examples for these are the European Council's Convention on Cybercrime adopted on 23 November 2001 (hereinafter Cybercrime Convention), Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (hereinafter Framework Decision), the Council of Europe Convention on the Protection of children against sexual exploitation and sexual abuse adopted on 25 October 2007 in Lanzarote[9] (hereinafter Lanzarote Convention), and the recommendation of the Committee on Civil Liberties, Justice and Home Affairs to the EP (hereinafter 2009 proposal for a EP recommendation).[10]

[9] Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse (CETS. No. 201 – 25. X. 2007)

[10] Committee on Civil Liberties, Justice and Home Affairs’ report with a proposal for a European Parliament recommendation to the Council on combating the sexual exploitation of children and child pornography (2008/2144(INI)) 26.01.2009; See also: European Parliament recommendation of 3 February 2009 to the Council on combating the sexual exploitation of children and child pornography (2008/2144(INI)) On 29 March 2010 the European Commission adopted a proposal for a new Directive on combating sexual abuse, sexual exploitation of children and child pornography. It follows up a previous proposal tabled in 2009. The Directive, if approved, will replace the Framework Decision 2004/68/JHA.

The Cybercrime Convention, the Framework Decision and the Lanzarote Convention regard all depictions of child sexual abuse as criminal. The objects of commission do not only include depictions of existing minors, but realistic images representing a minor, and also depictions of persons appearing to be a minor engaged in sexually explicit conduct.[11] Despite the above, the applicable law of different countries is not unified: not only visual or **graphic depictions**, but textual descriptions (Germany, see Sieber 1999), and voice recordings (answering machines) can be an act of commission too (Switzerland, see Suter-Zürcher, 2003). Hungary, where the act of commission of child pornography has a narrow definition only punishes the pornographic depiction of *existing* minors. At the same time, mainly in the youngest member states of the EU, such as Slovenia, Romania or Bulgaria, there is no clearly delineated legal practice concerning the acts of commission. (Parti, 2009)

In the past years, law enforcers have become increasingly interested in **virtual child sexual abuse,** the more spectacular, more interactive manifestation of the online sexual exploitation of children. Virtual child sexual abuse, also called ageplay is a sexual service which is – probably – offered by adult users to adult users. Virtual child prostitutes are available in virtual brothels, where there are playgrounds and children’s rooms in place for the purpose. The perpetrators, behind whom there are real adults, may enter into a sexual relationship with virtual children with the help of action balls. The client pays for the virtual sexual intercourse to the provider of the services (a kind of madam operating a brothel) in virtual money. The virtual currency is quoted in the stock exchanges of the real world, and it can be converted to real money. The fact that there are often other avatars present and watching the virtual act, shows how popular these ageplays are.

In relation to crimes and deviances against persons in the virtual world, the underlying question is, who and how is **harmed** by these acts, if the physical body is not hurt, and not even in any danger? If we apply this question to virtual child sexual abuse, we may ask what role does the fight against ageplay, if there is no contact crime, and even the user posing as a child is actually an adult?

The debate is ongoing on what effect exactly the ageplay may have on the participants. According to some, the participants act out their desires through the game, and would never touch real children, while others say that it only promotes habituation.[12] (Clark & Scott, 2009) Quayle & Taylor write that the use of online images of children has several functions. It is a means of justifying behaviour, a way of making children compliant by blackmailing them, as trophies, or even as a form of currency for exchange with other paedophiles. (Quayle & Taylor, 2002; Sullivan, 2007) There is no proof that behaviours practiced in the virtual world will ever manifest in the real world. On the other hand there is no guarantee that virtual contact really keeps participants back from committing the same in the geographical world. The contact between the virtual and real world, however, is shown undeniably by the fact that ageplay is not an isolated phenomenon. There are also identified paedophile rings present in virtual communities (e.g. Boy Love Online in Second Life) which are trading images of real children.

[11] Art. 9 § 2 of the Cybercrime Convention; Art. 1 § b./ of the Framework Decision, Art. 20 § 3 of the Lanzarote Convention

[12] Psychologist and psychotherapist Lutz-Ulrich Besser said about ageplay that it breaks down inhibitions, therefore gets the person closer to an offline act, that is a contact crime. Besser believes that ageplay is a playful preparation of the contact with a real child and the commission of an offline crime.

There are also problems surrounding the definition of child sexual abuse in practice. Neither the Framework Decision, nor the Lanzarote Convention gives a definition of images that '**visually depict'** children.[13] Member states prosecuting realistic depictions of non-existent children could not come at an agreement so far regarding the extent to which the realistic images should be recognisable. For example, does a hand drawing of a child qualify? To what an extent should the children in a hand drawing be recognisable? To what an extent should a computer-generated image be recognisable (e.g. computer animations, child characters in computer games or avatars appearing in virtual communities)? The question may be rephrased as 'where exactly do the boundaries of a **virtual child** lie'. (Parti, 2009) A German public prosecutor (Peter Vogt, Oberstaatsanwalt, Halle) says that if the action and the age of the characters intended to be depicted are both clearly recognisable (e.g. in the computer-animated world of Second Life), then a crime is committed, independent of the virtual space and the actual age of the users behind the child-avatars. (Second Life Insider, 2007) The reason why virtual depictions are criminalised is that online and offline forms of abuse can not be separated, since not only the depicted child, but any child can be a victim. The necessary steps must be taken for the protection of children's human dignity, and against the popularisation of sexual exploitation of children. (Quayle, 2010; Williams, 2010) From the point of view of the criminal theory, criminalisation of depictions of non-existent children involves anticipatory criminal liability to an early endangering of goods as a means of prevention. Anticipatory criminal liability is abstract regulation of a societal process, hence, it is already a risk management tool, because it punishes the possible future transformation of an act based on a weak causal interdependence. (Zavrsnik, 2007)

The Lanzarote Convention and the 2009 proposal for an EP recommendation would not only regard the actual sexual abuse, but also its related **preparatory behaviours as sui generis criminal acts.** Such behaviour is for example an online chat session with the intention of sexual exploitation, or any other forms of contacting children online with the aim of the child's sexual abuse.[14] The question is, how it can be evidenced that the child was contacted online in preparation of an actual act of abuse offline, if the actual abuse does not take place (at least it is not attempted). In some countries – for example the United Kingdom (2004)[15], Austria (2006)[16] and Bulgaria (2007)[17] – such acts are punishable as sui generis crimes. In other countries, legal regulations on online child grooming are in preparation. (For an overview of countries see ICMEC annual reports on Child Pornography: Model Legislation and Global Review)

There is no general legal practice as regards regulating the possession of images of child sexual abuse. The Cybercrime Convention does give member states the opportunity to leave the act of possession unpunished, and therefore fails to create unified conditions for the prosecution of international child sexual abuse networks. At the same time, it is not clear

[13] Art. 1, b./ of the Framework Decision; Art. 20 § 2 of the Lanzarote Convention

[14] Art. 23 of the Lanzarote Convention

[15] The Sexual Offences Act (2003, Section 15) introduced the punishemnt of meeting children online (not in person, but by mobile phone, chatrooms or similar), if such happens with the intention of offline (physical) sexual abuse. Offenders face up to 10 years of inprisonment. See online at: http://www.opsi.gov.uk/acts/acts2003/en/ukpgaen_20030042_en_1.htm

16 The Austrian anti-stalking law (§107a StGB) punishes grooming with inprisonment of up to one year. See online at: http://www.internet4jurists.at/gesetze/bg_stgb01.htm#%A7_105

17 Section 155a Subsection (1) Criminal Code of the Republic of Bulgaria (State Gazette 38/2007) See online at: http://www.legislationline.org/documents/section/criminal-codes

whether the temporary storage of data such as *cookies*, *cache* or *temporary files* directory qualifies as a means of intentionally acquiring the depictions. A further question is, whether the establishment of criminal liability may be technically dependent on restorability. Acquiring and possession are also behaviours, whose criminalisation is aimed at the prevention of an event (sexual abuse) that may occur in the future, which is, in practice, not always causally linked to acquisition and possession. (Zavrsnik, 2010)

The Lanzarote Convention extends the scope of punishable preparatory behaviours, e.g. the **access** – without downloading – of websites containing child sexual abusive images.[18] Here, however, a question of proof arises, namely how to distinguish technically between intentional downloading and unintentional access. At the moment, whether the perpetrator '**accessed'** the child sexual abuse contents out of negligence or intentionally, can only be proven with indirect evidence. Such indirect evidence may be for instance the magnitude of further child sexual abuse images recovered from the computer of the accusee, their classification into galleries, or whether the accusee visited websites containing child sexual abusive material regularly or not. (Krone, 2004; 2005) By any means, a proof of intentional access beyond any doubt is at the moment technically not feasible.[19]

Abstract endangering delicts are very **difficult to prove**. While the abuse is not in at least an attemptual phase, we can not prove the causal link to online contact. In relation to the abstract endangering delicts, the danger of a thought police or an authoritarian state which passes judgement over people's activities not on the basis of actions, but thoughts, is very real. A wide array of online surveillance technologies are available today for the control of criminality, but only at the detriment of private life and human rights. (Wykes & Harcus, 2010) This is why the authors Wykes and Harcus remark that if governments continue this surveillance, they themselves will become terror governments, and the countries they govern become terror states.

In recent times, the sphere of persons or institutions that can be made liable in relation to virtual child sexual abuse has been extended. The liability of not only those making depictions available, but also that of the Internet service providers arises. The 2009 proposal for an EP recommendation would regard all persons 'serving' Internet users showing an interest in child abuse as criminal, among them also those **operating online chatrooms and forums** dealing with sexual exploitation of children. The question remains, however, which chatrooms can be proven to be aimed at the sexual exploitation of children. Is it sufficient for example for someone to initiate such a conversation in a chatroom and not to be expelled from the chatroom, or will it be only chatrooms with conversations exlusively of such nature that meet the criteria, or will there have to be such a chatroom service affiliated with a website containing child sexual expoitation content?

In the recent years, solutions for the blocking and filtering of illegal content on the Internet appeared one after the other. These also represent a rather controversial area of **crime**

[18] Art. 20 § 1.f/ of the Lanzarote Convention

[19] The Lanzarote Convention entered into force in July 2010. Countries who adopted the regulations of the convention into their national law include Denmark, the Netherlands, Greece, and the signatories include member states of the European Union such as France, Germany and the United Kingdom. These states support the ideas of the Convention on symbolic legislation. For the list of ratifications and signatories see: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=8&DF=26/07/2010&CL=ENG

prevention. (See e.g. Sieber, 2009 on the debate surrounding German Internet-blocking efforts.) The government level control of the Internet is usually introduced under the aegis of the fight against online child sexual abuse, but it may be based on other delicts considered to be dangerous to the self or the public. The tools of content blocking on the Internet are not yet really effective, and can be by-passed with basic technical skills. On the other hand, the danger of overfiltering/overblocking is also realistic. This means that also some legal content is kept from the Internet users which infringes on such civic liberties as the freedom of access to information and fundamental rights such as the freedom of expression.

There are also moral, constitutional, debates, reconnaissance, and evidence difficulties related to **abstract endangering** crimes committed in an online environment. If the right to freedom of expression is a fundamental constitutional right, then on what grounds could the expression of an opinion be restricted which does not, only *may* pose a direct threat? What communication of how many users should be recorded for us to be able to prove the future intentional commission of the crime? If it is difficult to prove the intentional nature of the acquisition of illegal contents, than how will we prove that the attempts to groom a child had the final aim of sexual abuse – before any actual sexual abuse was attempted?

The international documents on the sexual exploitation of children clearly indicate legislative trends. They use criminal law to prevent the possible threat preceding the abstract threat – that is the anticipatory act of the crime. Criminal law may be a quick and simple response to a mass threat posing a great danger to certain layers of society (here minors) and can therefore be suitable to reassure society. It is another matter, whether this psychological tool achieves the goal of prevention in practice. Is it a necessary and proportionate tool for the prevention of such an abstract threat, and is criminal law really the most suitable means to reduce the threat?

The above mentioned legislative trends are influenced by the concerns communicated by the traditional media, the need for the protection of citizens (especially children), and the findings of scientific research. Therefore, legislation is shifting towards a detailed regulation which carries a couple of risks. Namely, there is a trap of overregulation, casuistic decisions, redundancy, and lack of transparency. There is also a troubling tendency of criminalising preparatory behaviours, due to the the fact that these are difficult to prove, and it is difficult to separate intentionality from negligence. Furthermore, due to overcriminalisation, criminal law becomes *prima ratio* instead of *ultima ratio*. Criminal law becomes the tool of primary reaction to milder deviances as well. This is a dangerous trend, especially if it is not coupled with other preventive tools, as information on safe Internet-use is scarce, and even parents are unaware of how they could prepare their children for the dangers of Internet-use. (Michelet, 2003; Mitchell et al., 2003; Kiesler et al., 2000; Turow & Nir, 2000)

5. Actual policing in virtual reality

Since in an ideal case, criminal law is only the last resort of regulators, let us see first what other means there are to fight harm and deviances in VR communities.

5.1 Self-regulation of virtual communities

The regulatory methods and bodies of virtual communities can be summarised as follows.

1. The community itself passes unwritten rules (informal rules: local ’customary law’ that is written law in the making).

2. The community itself introduces written regulations (formal rules, such as conduct and content guidelines, e.g. Terms of Service, End User Licence Agreement).
3. A few members of the community decide on the rules based on authority bestowed on them by the community (case-by-case judgement, establishment and execution of sanctions e.g. expulsion from the community).
4. Internet Service Provider (ISP): the user accepts (registration) and regards as binding to himself the rules of the ISP when joining the community (when these rules are breached, the ISP may suspend or block the IP-address belonging to the given account, and in more severe cases may report to the authorities).
5. In the case of the gravest deviances (which cause great harm and are inevitably punishable under offline legal regulations), an external authority (investigative authority, jurisdiction) has competence on a national level.
6. Supranational level: the foundations of international cooperation are laid by international conventions and other documents. (For a general overview see Wall, 2001)

Virtual communities regulate primarily themselves with a set of regulations created from the bottom up (self-regulation**). Self-regulation** is a form of **informal social control** which the members of the community practice over rule-breakers. In the early stages of virtual worlds, the only regulator was the **system administrator**, who suspended or expelled members with technical means. This rather oligarchic system of regulation did not observe the interests of the community or the opinion of the community members, and could only work in smaller communities, where the control through the administrator was still effective. However, the continuous growth, democratic nature and zero-tolerance approach towards deviances of virtual communities lead to more mature regulations. This then resulted in the appearance of self-regulation and vigilante groups. The increasingly widespread organised activities of vandalistic groups demand a more serious defence and preparation from the community. One of the possible means of action against such organised attacks can be the vigilante groups, consisting of volunteering, independent 'policemen' (such a vigilante group in the virtual space Cyberworlds is Peacekeepers, see Williams, 2006). The tasks of vigilantes include the qualification of acts, sanctioning, the temporary ejection from the world, and account suspension or ultimate cancellation. The vigilantes' sheer presence has a preventive role, and increases the sense of security in the residents. (Crawford & Lister, 2004) If the vigilantes fail to reach their goal, the victim may report the attack at the ISP, who will warn the attacker to put an end to his behaviour, and suspend or block him from further participation. Users may also take action against the attacker individually by reporting him to the service provider (by sending an abuse report).[20] **If there is a more serious breach of rules,** the community may vote the attacker off from among the residents (ostracism). (Talin, 2003) Voting off from the community is based on the principle of shaming. Shaming functions as a punishment, and relies on the principle of conditioning which we learn at a young age. (Braithwaite, 1989) It teaches people to tell apart good and bad, and to feel guilty, if we think we have done something wrong. As the feeling of shame is an internal reaction (and not an external command), it has an immediate, and therefore educational effect. (Hirschi, 1969) Braithwaite says that the

[20] E.g. the Second Life Terms of Service says that 'big six transgressions', that is intolerance, harassment, assault, disclosure (of personal information), indecency and disturbing the peace may prompt an abuse report to Linden.

individual usually has the impulse to commit the crimes, but the stronger his ties to the (virtual) community, the greater the restraining effect. (Braithwaite, 1989)

The system of rules of virtual communities always corresponds to the needs of residents and is heterogenous. The governing is namely not practiced by a higher body, but the community based on organic rules, or a by a group of residents appointed by the community. Boellstorff calls this governance system 'grassroot governance'. (Boellstorff, 2008) Belonging to a virtual community may already in itself have a preventive function. The humiliation used by virtual communities may have a stronger restraining effect than the sanctions of geographical communities, since the bonds within a virtual community, as we have seen, may be stronger. However, community governance is also criticised.

The **administrator** represents his own selfish interests and not the community by setting the rules of joining the community, and judging the breaches of rules alone (dictatorship). (Doctorow, 2007; Chun, 2006) **Vigilantes** are effective in repelling systematic attacks destructive for the community, but are less effective in fighting sporadic, ad-hoc individual actions. The vigilantes are unable to act directly on the scene of the crime which means that action and sanction are separated in time. (Williams, 2010) **Abuse reports** sent by residents to the administrator carry the risk of another abuse, as they may contain false accusations which may lead to a tarnished reputation, account suspension, or financial losses even if the accusations are proven to be unfounded. If the reputation is tarnished disproportionately by the abuse report as compared to the damage caused, the abuse report is deviant, independent of whether it was at least partly justified or not. (Boellstorff, 2008)

Lessig says that **technology** is a more effective means of governance than legal regulations, norms or even community tools. (Lessig, 1999) This is the essence of the Internet, and regulation should also be based on this. The key to its effectiveness is that it can change the 'behaviour of avatars', can stop them from continuing their subversive behaviour, can be easily adjusted to the community's needs, can be a means of prevention and more than just a response to deviances (e.g. if the platform developer does not make certain behaviours possible). As it is automated, it is an invisible means of control, and does not give residents the feeling of being constantly watched and controlled. (Williams, 2006) Besides that, only technology makes immediate response possible. Lessig's main argument, however, is that technology does not rely on individual judgement, and there are no abuses of power. Technology is the most effective means of regulation, since it is liberal, equal and can be developed. Some critics say however, that even technical regulation can not be objective, as the system's crack-proofness always depends on the creativity of the code writers. Therefore technical design is also permeated by subjectivity. (Hosein et al., 2003)

5.2 Formal control of virtual communities – police presence

Eventhough there are only guesses as to the nature of threats, and estimates for their volume, and the criminal law assessment of preparatory acts is much debated, the presence of the police forces in VR communities is very real. While virtual communities solve the problem of crime prevention with their own internal control (**informal control**), geographical authorities carry out their criminal prosecution and preventive activities in a form approved by the state (**formal control**).

The presence of police organs in virtual communities on the one hand can raise the sense of security in virtual citizens, and on the other it is suitable for the surveillance of the life of virtual alteregos, and thereby for the discovery of crimes in an early stage through covert investigative measures.

Several countries maintain a police unit in virtual communities. One of the biggest both in terms of scope of action and the number of cooperating partners, is the London-based Child Exploitation and Online Protection Centre (CEOP)[21] which also carries out investigations in online environments to uncover child sexual abuse. CEOP cooperates with several police units and foreign police forces in the UK and abroad, because transnational crimes committed on the Internet demand international cooperation. CEOP has a central role in receiving and forwarding information. CEOP has the responsibility in the UK for receiving intelligence and information from overseas on child sexual abuse crimes. CEOP's Intelligence Faculty analyses and develops the material that they receive from other organisations and forwards details of individual suspects to local police forces, who in turn initiate their own investigations. CEOP's officers are technically the officers of the Serious Organized Crime Agency (SOCA). SOCA also has a Paedophilia Unit, but CEOP is an independent coordinator of online investigations into paedophilia cases.

CEOP does not only act as an investigative authority, but also makes considerable efforts in the fields of primary prevention, and informing the population about threats[22]. It also maintains a reporting centre, and keeps the knowledge of experts up-to-date with continuous trainings.

Other countries' police authorities are not directly present in virtual communities, that is they do not monitor communities directly, but may initiate criminal proceedings, if they acquire information on crimes committed in a virtual space. The German investigative television channel ReportMainz looked into the child sexual abuse scandal around Second Life. They found that the German Federal Criminal Police Office (Bundeskriminalamt) was informed by CEOP in early 2007 that in the virtual world of Second Life sexual services of child avatars are sold at brothels (that is children are forced into prostitution). There were German citizens among the offenders, who accessed the virtual community through German servers. The detectives of the Federal Criminal Police Office entered the virtual community, and together with the undercover detectives of CEOP uncovered the criminal ring. (Report Mainz, 2007; see also CEOP Center film, 2009) The administrator of Second Life, Linden Lab agrees to cooperation with investigative authorities, but the users' statement accepted when entering also stipulates that no acts may be committed in Second Life that would constitute crimes in the geographical world, and they expressly refer to the ban on abuse against children. What is more, they also ask users to report any such abuse they encounter to the International Centre for Missing and Exploited Children (ICMEC). They have also announced that they intend to develop a system that would prevent such abuse. How they would do it, remains a question.

The government bodies and the military of the US are also present in Second Life, where they possess islands. (Au, 2005) With the spread of the trade with virtual goods, there has been an extension of state power to virtual communities in recent times. The European Union levied a tax on its citizens who are residents in Second Life, and have an account in the virtual world. The residents pay tax after real and movable estate that they directly buy from the developer of the platform, Linden Lab.[23] The US Congress discussed a possible tax

[21] CEOP also maintains a website, http://www.ceop.gov.uk

[22] For CEOP's awareness-raising campaign see http://www.thinkuknow.co.uk

[23] Anything that a resident pays for to Linden Lab has VAT added. This includes premium account registration, purchases from the Land Store, land use fees (tier), Private Region fees, land auctions, LindeX transaction fees. (WikiSecondlife on VAT, 2010)

on Second Life residents after their income and property there, and also a possible intervention of the US authorities in the regulation of contents. (NeoWin, 2009) Boellstorff believes that this is bound to be the most debated issue in relation to VR communities in the future.

Eventhough most police organs are not directly present in virtual communities, they are carrying out investigations in relation to crimes in virtual worlds within the framework of international cooperation. Therefore Europol, the police cooperation organisation of the European Union, and the coordinator of international cooperation, Eurojust both have a significant role in uncovering crimes committed online. (See for example Operation Koala: CEOP press release, 2007)

5.3 Outsourcing of formal control

In recent times, there is a visible trend for state crime prevention activities (**formal control**) to be outsourced. More and more, the state's crime prevention role is taken over by NGOs, and the police also involve NGOs in their criminal prosecution activities (thereby strengthening informal control).

The reason for the outsourcing of state criminal prosecution activities is on the one hand the continuous specialisation of technical skills related to the Internet, and on the other the decentralisation of the state. (Yar, 2010) The concept of the traditional economic and social welfare state failed in the second half of the 20th century. The state is trying to perform these tasks traditionally in its own sphere of responsibility in that it hires NGOs for the purpose. Such tasks include containing crime, and also prevention. The decentralisation of the state is based on a neoliberal philosophy which gradually liberalises and deregulates markets, and privatises the public sphere. This has the advantage that costs are shared among those in charge of different tasks, and it also frees public agencies – such as the police force – from the burden of responsibility and the tasks in the ever expanding field of crime prevention. The growing rate of privatisation of the control of online crimes and its acquisition of economic players is a result of this neoliberal process. It was high time, as the police are not achieving any apparent results in the field of investigations into and the procesution of Internet crime against significant financial investments. (Wall, 2001)

Decentralisation not only shows in the outsourcing of criminal prosecution, but also that of crime prevention activities. The moral panic that the state made good use of and in certain cases artificially generated to shape the self-protection mechanisms of citizens has backfired. Citizens' fear of crime has become irrational. Füredi even speaks of a fear of fear itself (Füredi, 1997) which manifests in that citizens are overly afraid, and even panic when it comes to crimes, irrespective of whether there is an actual threat. (Wall, 2010) This is also mentioned in Garland's crime complex, where he says that we expect crime on a large scale, and go into a state of shock if we do not encounter it. (Garland, 2001) The fulfilment of crime prevention tasks – awareness raising, crime and subcrime reporting, victim assisting – is transferred more and more to user communities. User communities are self-regulating communities, hence they decide themselves what needs protecting and how, and what the means of protection should be.

According to Yar's classification, there are criminal prosecution organs participating in the regulation of the Internet which belong to the non-governmental area. On the other hand, commercial players carrying out profit-oriented policing activities have a great role to play in regulation. (Yar, 2010) Such is for example the awareness-raising activity of software manufacturers, or their contribution to containing online crime. An example for this is the Child Exploitation Tracking System (CETS) developed by Microsoft Corporations in 2005 for the tracking of online child sexual abuse offenders. The application based on Microsoft's technology is used by investigative authorities across the world to track the online movements of suspected offenders and to collect evidence without accidentally performing the same work twice.[24] This example shows well that external players are needed in criminal prosecution not only due to the growing number of tasks, and the insufficiency of state competencies, but also rapid technical development. The more the investigative authorities are unable to keep pace with technical development, the greater and more important the role of business organisations in the field of criminal prosecution.

For investigations in virtual worlds, the cooperation of the platform operator or the Internet service provider with investigative authorities is very often necessary for technical reasons. The platform operator, who is actually the system administrator, is the lord over virtual worlds. He has the log-in and other personal data of the suspected offender, without which the investigative authorities could never track down the offenders. (In the case of Second Life, Linden Lab cooperates with the authorities of the geographical world in reconnaisance activities. They establish who are behind the avatars committing crimes in the sense of geographical law, and put the user accounts at the disposal of investigative authorities.) A good example for the cooperation of Internet service providers is the application of solutions developed for the filtering and blocking of illegal and harmful online content. (Sieber & Nolde, 2008; Tous, 2009) Governments have the option of several different solutions for filtering illegal or harmful content. All of them are based on the principle that the main ISPs active in the given country should filter the content passing through their servers based on certain considerations, so that these do not get to the users. ISPs however also have an obligation to report to investigative authorities if they encounter illegal content. The Cybercrime Convention and the Data Retention Directive of the European Union prescribe a similar obligation for the ISPs in relation to the storage and forwarding to the investigative authority of traffic data.[25] Service provider cooperation plays an important part in each document, as data from ISPs serve as evidence in criminal proceedings.

The need for the private regulation of the Internet is natural. It is the interest of users and user communities to protect what they consider valuable and threatened, independent of priorities defined by the state. (For more on top-down initiative and consensus based processes see Castells, 2002) Several such citizens' initiatives of crime prevention developed in relation to the fight against online child abuse. Such is for example Internet Watch Foundation (IWF)[26] which was established in 1996 in the United Kingdom. IWF is a self-regulating system consisting of the representatives of content providers and telecommunication companies. Its method is the monitoring of online content. They are

[24] For more see: http://www.microsoft.com/industry/publicsector/government/cetsnews.mspx

[25] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications and the modification of directive 2002/58/EC (Data Retention Directive) (OJ L 105/54-63)

[26] IWF: http://www.iwf.org.uk

primarily fighting online child abuse, hate speech and racist content, and maintain a hotline for reports by the public. They compile a blacklist of non-desirable contents which several ISPs have adopted, and on the basis of which they remove content. Working To Halt Online Abuse (WHOA)[27] is a similar initiative started in 1997, and fighting against Internet harassment and assault. The International Association of Internet Hotlines (INHOPE)[28] was established in 1999, and defines and unifies the description of illegal and harmful online content, maintains reporting hotlines in 42 countries around the world, and also provides the public with advice adjusted to local conditions (helpline and awareness raising) on safe surfing. The organisation Cyberangels, mainly involved in awareness raising, was established in 1995, based on the example of Guardian Angels started in the US to fight street crime.[29] Cyberangels draws attention to the latest online crime trends, offers protection solutions to users in the case of online stalking, helps avoid identity theft and maintain online privacy. The Association of Sites Advocating Child Protection (ASACP)[30] is a certification association of pornographic websites registered in the US, and has been watching over the legality and compliance of pornographic content using the labelling technology since 1996. This organisation also has a hotline to promote the legal awareness of users.

The investigative authorities also cooperate with several service providers of online platforms to detect crimes. A recent example to this is a statement made by Facebook in July 2010 that they would add a Facebook Panic Button to the website. Facebook already allows its users to report online attacks against them, but the Panic Button would expressly be dedicated to reporting child sex abuse. The user would be able to send his report directly to CEOP by klicking the Panic Button. (CEOP press release, 2010) Besides child protection, there are a number of non-governmental organisations working in other fields, such as the freedom of speech and expression, privacy protection, and the free movement of information.

A virtual community is ideally regulated and governed from within, by itself (informal control). Formal (geographical) control is for many reasons not desirable. If the state once starts to restrict the freedom of speech – first only for reasons of fighting illegal and harmful content –, there is no guarantee that the restriction of civic liberties will stop at that. The state's demand for exerting criminal law clashes with civic liberties.

Virtual communities have grassroot governance, and no external, formal control fits into this system either from a technical, or a social structure point of view. Formal control has an effect that evolves towards the restriction of members' rights and is disruptive of the community. The rules of geographical authorities do not fit into the decentralised system of virtual communities. The Internet is transnational, and its nature does not allow any independent power to impose dedicated rules on it. What is more, the assessment of contents can be different in different jurisdictions, but the Internet does not distinguish between users on the grounds of their nationality, or what geographical law is applicable to any given user. (Williams, 2010; Boyle, 1997)

[27] WHOA: http://www.haltabuse.org/

[28] INHOPE: https://www.inhope.org/

[29] Cyberangels: http://www.cyberangels.org/security/index.php

[30] ASACP: http://www.asacp.org/

There may be concerns in relation to the activities of 'external', non-police organisations that they represent their own interests better, than those of the community. So for example manufacturers of content filter software have less interest in protecting consumers than in generating profit, and responding to the requirements of the marketplace. (Yar calls this democratic deficit: Yar, 2010)

6. Conclusion

In the 1990s, computer-mediated communication was judged without empirical research. But even today, we know relatively little about crimes and deviance occuring in the virtual world. (Williams, 2010)

Virtual worlds are not merely copies of the geographical world. Actual world computers and flesh and blood bodies are needed for their existence, and they possess a lot of elements of actual society. Through technology, residents can recreate their world in a way that nobody today can predict, since it is the first time in history this is happening. (Boellstorff, 2008)

There is need for research on the validity of criminological theories online (Williams, 2006) and how these communities could be regulated more effectively. Further concepts should be elaborated on what combination of formal, informal and technical control can effectively curb and give a response to offences.

Moral panic which only intensifies with the development of online communities, has an effect both on the degree of detail of legislation and the intensity of police intervention. The action of the authorities of the geographical world is absolutely necessary in relation to the gravest and most widespread acts. However, imposing rules on the communities is mainly the task of the comminities themselves. The decentralised technical structures of the Internet do not make it possible for an external entity to shape the rules to be followed. Attempts should be appreciated of course, and the state's efforts to exert criminal law are also understandable, as their aim is the protection of national security and the citizens. We should, however, concentrate on three important expectations.

The first one is that legal **regulations should be transparent and easy to follow**. In virtual communities, some activities are not realised as in real space, and the harm or actual threat they pose are not direct counterparts of geographical harms and threats, for which reason the prosecution of these acts in the virtual world is questionnable.

The second requirement is that criminal law should remain in its traditional role as **ultima ratio**. Criminal law should not be the primary means to curb virtual deviances. Legal regulations should be supplemented with preventive measures at government level, such as for example raising awareness of threats, school education, and public information campaigns.

The third very important criterion is **adjusting the approach of law enforcement to the virtual space**. This does not only mean the continuous technical training of law enforcement officers, but also the learning of an analytical approach which would help law enforcement understand the events of virtual communities, namely who does what and why in the virtual world. Knowledge of the virtual community teaches us to identify in what situations there is a real threat, and identify the preparatory behaviours of actual cimes. We should however also remember that correlation between events does not equal causality.

7. References

ABCNews.com, 2000: 'Barrel Killings Suspect Charged Again' 28 July 2000 *ABCNews.com* Available at: http://abcnews.go.com/US/story?id=96339&page=1; [15/05/2010]

Au, W.J. (2005). 'The Tragic of Tringo' *New World Notes'* 8 March, 2005 Available at: http://nwn.blogs.com/nwn/2005/03/the_tragics_of_.html [30/07/2010]

Austin, J.L. (1975). *How To Do Things With Words: [2nd ed.]* Harvard University Press ISBN 978-0-674-41152-4 Cambridge, MA

Becker, P.J., Byers, B. & Jipson, A. (2000). The contentuous American debate: the first Amendment and Internet-based hate speech. *International Review of Law, Computers, and Technology,* Vol. 14, No. 1: 33-41 ISSN 1364-6885

Bell, D. (1999) [1993]. *The Coming of Post-Industrial Society [3rd ed.]* Basic Books ISBN 0-465-01281 New York

Bocij, P. (2004). *Cyberstaling: Harassment in the Internet age and how to protect your family.* Praeger ISBN 0-275-98118-5 Westport, Connecticut, London

Boellstorff, T. (2008). *Coming of Age in Second Life.* Princeton University Press ISBN 978-0-691-13528-1 Princeton & Oxford

Boyle, J. (1997). Foucault in Cyberspace: surveillance, sovereignty and hard-wired censors. *University of Cincinnati Law Review*, Vol. 66 No. 2: 177-205 Available at: http://www.law.duke.edu/boylesite/foucault.htm [30/07/2010] ISSN 0009-6881

Braithwaite, J. (1989). *Crime, Shame and Reintegration*, Cambridge University Press ISBN 0-521-35668-7 Cambridge

Butler, J. (1997). *Excitable Speech:: A Politics of the Performative.*, Routledge ISBN 0-415-91587-2 London

Casey, E. (Ed.) (2004). *Digital evidence and computer crime. Forensic science, computers and the Internet [2nd ed.]* Elsevier Academic Press ISBN 0-12-163104-4 San Diego, CA

Castells, M. (2002). *The Internet Galaxy: Reflection on the Internet, Business and Society,* Oxford Univesrity Press ISBN 3-8100-3593-9 Oxford

CEOP Center film, 2009: *'Victim Identification'* Available at: http://www.youtube.com/watch?v=CTvufchSYMs [30/07/2010]

CEOP press release, 2007: *'46 Arrests in UK as international child sex offender network smashed'* 5 November 2007 Available at: http://www.ceop.police.uk/mediacentre/pressreleases/2007/ceop_05112007.asp; [27/07/2010]

CEOP press release, 2010: *'Facebook and CEOP get 'appy. Facebook and CEOP join forces to deliver internet safety to young internet users'* 12 July 2010 Available at: http://www.ceop.police.uk/mediacentre/pressreleases/2010/ceop_12072010fb.asp; [28/07/2010]

Chun, W. (2006). *Control and Freedom: Power and Paranoia in the Age of Fiber Optics,* MIT Press ISBN 978-0-262-03332-9 Cambridge, MA

Clark, N. & Scott, P.S. (2009). *Game addiction: The experience and the effects,* McFarland & Co. ISBN 978-0-7864-4364-2 North Carolina, US

Curtis, P. (1992). Mudding: Social Phenomena in Text-Based Virtual Realities, In: *Culture of the Internet*. Kiesler, S. (Ed.) 121-42 Lawrence Erlbaum Associates. ISBN 0-8058-1635-6 Mahwah, NJ

Delgado, R. (1993). Words that wound: A tort action for racial insults, In: *Words That Wound: Critical Race Theory, Assaultive Speech, And The First Amendment.* Matsuda, M.J., Lawrence, C.R., Delgado, R. & Crenshaw, K.W. (Eds.): 131-40 Westview Press ISBN 978-0-813-38428-3 Boulder, CO

Dibbel, J. (1998). *'A Rape in Cyberspace'* Available at: http://www.juliandibbell.com/articles/a-rape-in-cyberspace/; [02/05/2010]

Doctorow, C. (2007). 'Why Online Games are Dictatorship?' *Information Week* 16 April, 2007 Available at: http://informationweek.com/internet/showArticle.jhtml?articleID=199100026&pgno=1&queryText=; [01/05/2010]

Foo, C.Y. (2004). Redefining Grief Play. *Proceedings of the Other Players conference,* Copenhagen, Denmark. Available at: http://www.itu.dk/op/papers/yang_foo.pdf [27/10/2006]

Füredi, F. (1997). *Culture of Fear*, Continuum ISBN 0-304-3375-1 London

Garland, D. (2001). *The Culture of Control*, Oxford University Press ISBN 0-19-829937-0 Oxford

Harmon, D. & Boeringer, S.B. (1997). A content analysis of internet-accessible written pornographic depictions, *Electronic Journal of Sociology,* Available at: http://www.sociology.org/content/vol003.001/boeringer.html [18/07/2010] ISSN 1198-3655

Hirschi, T. (1969). *Causes of delinquency.* University of California Press ISBN 978-0-765-80900-1 Berkeley, LA

Hosein, G., Tsavios, P. & Whitley, E. (2003). Regulating architecture and architectures of regulation: Contributions from information systems, *International Review of Law, Computers and Techology,* Vol. 17 No. 1: 85-97 ISSN 1360-0869

ICMEC annual reports on Child Pornography: Model Legislation and Global Review, 2008, Alexandria, Virginia: USA, Available at: http://www.icmec.org/en_X1/English__5th_Edition_.pdf; [19/06/2010]

Innes, M. (2004). Reinventing tradition? Reassurance, neighbourhood security and policing, *Criminology and Criminal Justice* Vol. 4 No. 2: 151-71 ISSN 1748-8966

Jenkins, P. (1998). *Moral Panic. Changing concepts of the child molester in modern America.* Yale University Press ISBN 0-300-07387-9 New Haven & London

Joinson, A.N. (2003). *Understanding the Psychology of Internet Behaviour*, Palgrave Macmillan ISBN 0-333-98467-6 London

Kiesler, S., Zdaniuk, B., Lundmark, V. & Kraut, R. (2000). Troubles with the Internet: The dynamics of help at home, *Human-Computer Interaction*, Vol. 15 No. 4: 323-51 ISSN 1532-7051

Korinek L. (2006). *Bűnözési elméletek. [Theories on Offending]* Duna Palota és Kiadó ISBN 963-8036-97-4 Budapest

Krone, T. (2004). A Typology of Online Child Pornography Offending. Trends and Issues in Crime and Criminal Justice, *Leaflet of Australian Institute of Criminology,* No. 279 (June 2004) ISSN 1836-2206 Canberra

Krone, T. (2005). Does Thinking Make it so? Defining Online Child Pornography Possession Offences. Trends and Issues in Crime and Criminal Justice, *Leaflet of Australian High Tech Crime Centre*, No. 299 (April 2005) ISSN 1836-2206 Canberra

Lessig, L. (1999). *Code and Other laws of Cyberspace*. Basic Books 978-0-465-03913-5 New York

MacKinnon, C.A. (Ed.) (1997). *In Harm's Way: The Pornography Civil Rights Hearings,* Harvard University Press, ISBN 0-674-44578-3 Cambridge, Mass.

MacKinnon, R.C. (1997). Virtual rape, *Journal of Computer-Mediated Communication*, Vol. 2 No. 4, Available at: http://www3.interscience.wiley.com/cgi-bin/fulltext/120837717/HTMLSTART [16/08/2009] ISSN 1083-6101

Mann, D., Sutton, M. & Tuffin, R. (2003). The evolution of hate: social dynamics in white racist newsgroups, *Internet Journal of Criminology*, Available at: http://www.flashmousepublishing.com [21/06/2009] ISSN 1198-3655

Matsuda, M.J., Lawrence, C.R., Delgado, R. & Crenshaw, K.W. (1993). *Words That Wound: Critical Race Theory, Assaultive Speech, and The First Amendment,* Westview Press ISBN 978-0-813-38428-3 Boulder, CO

Markham, A.N. (1998). *Life Online: Researching Real Experience in Virtual Space,* Altamira Press ISBN 978-0-761-99030-7 Walnut Creek, CA

Mehta, M. D., & Plaza, D. E. (1997). Pornography in cyberspace: An exploration of what's in Usenet, In: *Culture of the Internet*, Kiesler, S. (Ed.): 53-67 Lawrence Erlbaum ISBN 0-8058-1635-6 Mahwah, NJ

Meloy, J. (1998). The psychology of stalking In: *The psychology of stalking: Clinical and forensic perspectives,* J. Meloy (Ed.):. 2-21 Academic Press ISBN: 0-12-490560-9 San Diego, CA

Michelet, I. (2003). *Our Children at Risk Online: The Example of Thailand.* A Survey Report. ECPAT International & UNICEF: 7-43 Available at: http://vac.wvasiapacific.org/downloads/ecpat2.pdf; [12/02/2008]

Mitchell, K.J., Finkelhor, D. & Wolak, J. (2003). The exposure of youth to unwanted sexual material on the internet. A national survey of risk, impact, and prevention, *Youth & Society,* Vol. 34, No. 3: 330-58 ISSN 1552-8499

Moitra, S.D. (2003). *Analysis and Modelling of Cybercrime: Prospects and Potential,* Research in Brief, Max Planck Institute for Foreign and International Criminal Law ISBN 3-86113-145-5 Freiburg

Mulligan, J. & Patrovsky, B. (2003). *Developing Online Games: An Insiders Guide,* New Riders ISBN 978-1-592-73000-1 Indianapolis

Murff, K. N. (2007). *Digital Crime Investigation Trends in State and Local Law Enfircement,* UMI Dissertation Services, UMI Number: 3294390 (No ISSN) Ann Arbor, Michigan, USA

NeoWin, 2009: 'IRS to tax Second Life/World of Warcraft earnings' 14 January 2009 *NeoWin* Available at: http://www.neowin.net/news/irs-to-tax-second-lifeworld-of-warcraft-earnings-3; [30/07/2010]

Oldenburg, R. (1999). *The Great Good Place,* Marlowe & Co. ISBN 1-6924-681-5 New York

Ondrejka, C.R. (2004). Escaping the Guilded Cage: User Created Content and Building the Metaverse, *Social Science Reserach Network Online* Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=538362; [12/07/2010]

Parti, K. (2009). *Gyermekpornográfia az interneten [Child pornography on the Internet]* Bíbor Kiadó ISBN 978-963-9634-92-3 Miskolc

Parti, K. (2010). Alterations in danger-awareness due to the infocommunication revolution and its effect on legislation, In: *Current Issues in IT Security. Proceedings of the interdisciplinary conference 12-14 May, 2009* Bellini, M., Brunst, P. & Jähnke, J. (Eds.): 91-105 Duncker & Humblot ISSN 1860-0093 Berlin

Quayle, E. (2010). Child pornography. In: *Handbook of Internet Crime*, Yar, J. & Jewkes, Y. (Eds.): 343-68 Willan Publishing ISBN 978-1-84392-524-8 USA & Canada

Quayle, E. & Taylor, M. (2002). Paedophiles, pornography and the Internet: Assessment issues *British Journal of Social Work*, Vol. 32 No. 7: 863-75 ISSN 0045-3102

Reid, E.M. (1999). Hierarchy and power: Social control in cyberspace, In: *Communities in Cyberspace*, Smith, M.A. & Kollock, P. (Eds.): 107-33 Routledge ISBN 0-415-19139-4 London

Reno, J. (1999). Cyberstalking: *A new challenge for law enforcement and industry*, U.S. Department of Justice: Washington, DC, Available at: http://www.justice.gov/criminal/cybercrime/cyberstalking.htm [01/12/2009]

Report Mainz, 2007: *'Kinderpornographie in Second Life'* Available at: http://www.youtube.com/watch?v=dynfVtC8Gt4; [27/07/2010]

Reynolds, R. (2005). *'The Four Worlds Theo*ry' Available at: http://terranova.blogs.com/terra_nova/2005/08/the_four_worlds.html; [13/07/2010]

Rimm, M. (1995). Marketing pornography on the information superhighway: a survey of 917,410 images, descriptions, short stories and animations downloaded 8.5 million times by consumers in over 2,000 cities in forty countries, provinces and territories, *The Georgetown Law Journal*, Vol. 83 No. 5: 1849-934 ISSN 0016-8092

Schechner, R. (1988). Playing, *Play and Culture*, Vol. 1, No. 1: 3-20 ISSN 0894-4253

Second Life Insider, 2007: 'Transcript of the German piece about age play' *Second Life Insider*, 11 May 2007, Available at: http://www.secondlifeinsider.com/2007/05/11/transcript-of-the-german-piece-about-age-play/; [21/07/2010]

Sieber, U. (2009). Sperrverpflichtungen gegen Kinderpornografie im Internet, *Juristen Zeitung* Vol. 64 No. 13: 653-62 ISSN 0022-6882

Sieber, U. & Nolde, M. (2008). *Sperrverfügungen im Internet,* Dunkel & Humblot ISBN 978-3-86113-861-7 Berlin

Simon, J. (2007). *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear,* Oxford University Press ISBN 0-19-518108-5 New York

Sullivan, J. (2007). Abuse spiral. *Presentation, proceeded at the Child Exploitation and Online Protection Centre Training*, Bucharest, 11-17 November 2007

Suter-Zürcher, S. (2003). *Die Strafbarkeit der sexuellen Handlungen mit Kindern nach Art. 187 StGB.* Universität Zürich ISBN 3-7255-4640-1 Basel-Genf

Taipale, K. (2006). Why can't we all get along: how technology, security and privacy can coexist in the digital age, In: *Cybercrime: Digital Cops in a Networked Environment*, Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. (Eds.): 151-83: New York University Press ISBN 0-8147-9983-3 New York

Talin (2003). Managing Deviant Behaviour in Online Worlds, In: *Developing Online Games: An Insider's Guide*, Mulligan, J. & Partovsky, B. (Eds.): 347-60 New Riders ISBN 978-1-592-73000-1 Indianapolis

Tous, J. (2009). Government filtering of online content, *E-Newsletter on the Fight Against Cybercrime (enac),* Vol. 1 No. 2: 14-20 ISSN 2013-5327

Turkle, S. (1995). *Life on Screen: Identity in the Age of the Internet*, Weidenfeld & Nicolson ISBN 0-684-80353-4 London

Turow, J. & Nir, L. (2000). *The Internet and the family 2000: The view from parents, the view from kids*, University of Pennsylvania, Annenberg Public Policy Center: Philadelphia, Available at: http://www.eric.ed.gov/PDFS/ED448874.pdf; [23/02/2008]

Wall, D.S. (2001). Maintaining order and law on the Internet, In: *Crime and the Internet,* Wall, D.S. (Ed.): 167-83 Routledge ISBN 0-415-24429-3 London

Wall, S.D. (2007). *Cybercrime: The Transformation of Crime in the Information Age,* Polity Press ISBN 978-0-7456-2735-9 Cambridge

Wall, D.S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime, *International Review of Law Computers & Technology* Vol. 22 Nos. 1–2: 45–63 ISSN 1610-7608

Wall, D.S. (2010). Criminalising cyberspace: The rise of the Internet as a 'crime problem', In: *Handbook of Internet Crime* (op.cit.): 88-102

WikiSecondlife on VAT, 2010:
http://wiki.secondlife.com/wiki/Linden_Lab_Official:Value_Added_Tax_(VAT)_Frequently_Asked_Questions#In_general.2C_who_should_be_charged_VAT.3F; [12/07/2010]

Williams, M. (2004). Understanding King Punisher and his order: Vandalism in a virtual reality community – motives, meanings and possible solutions, *Internet Journal of Criminology,* No ISSN, Available at:
http://www.internetjournalofcriminology.com/Williams%20-%20Understanding%20King%20Punisher%20and%20his%20Order.pdf; [12/07/2010]

Williams, M. (2006). *Virtually Criminal. Crime, Deviance and Regulation Online*, Routledge ISBN 978-0-415-36404-1 London & New York

Williams, M. (2010). The virtual neighbourhood watch: Netizens in action, In: *Handbook of Internet Crime* (op.cit.): 562-80

Wykes, M. (2010). Harm, suicide and homicide in cyberspace: Assessing causuality and control, In: *Handbook of Internet Crime* (op.cit.): 369-94

Wykes, M. & Harcus, D. (2010). Cyber-terror: construction, criminalisation and control, In: *Handbook of Internet Crime* (op.cit.): 214-29

Yar, M. (2010). Private policing of Internet crime, In: *Handbook of Internet Crime*, Yar, J. & Jewkes, Y. (Eds.): 546-60 Willan Publishing ISBN 978-1-84392-524-8 USA & Canada

Zavrsnik, A. (2007). Virtual child pornography: The concept of a pseudo-photograph. *Presentation proceeded at 7th Annual Conference of the European Society of Criminology,* Bologna, 26-29 Sept, 2007

Zavrsnik, A. (2010). Criminal Justice Systems' (Over)Reactions to IT Security Threats, In: *Current Issues in IT Security. Proceedings of the interdisciplinary conference 12-14 May, 2009* (op.cit.): 117-40

Virtual Reality

Edited by Prof. Jae-Jin Kim

ISBN 978-953-307-518-1

Hard cover, 684 pages

Publisher InTech

Published online 08, December, 2010

Published in print edition December, 2010

Technological advancement in graphics and other human motion tracking hardware has promoted pushing "virtual reality" closer to "reality" and thus usage of virtual reality has been extended to various fields. The most typical fields for the application of virtual reality are medicine and engineering. The reviews in this book describe the latest virtual reality-related knowledge in these two fields such as: advanced human-computer interaction and virtual reality technologies, evaluation tools for cognition and behavior, medical and surgical treatment, neuroscience and neuro-rehabilitation, assistant tools for overcoming mental illnesses, educational and industrial uses In addition, the considerations for virtual worlds in human society are discussed. This book will serve as a state-of-the-art resource for researchers who are interested in developing a beneficial technology for human society.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821