

Crime Potential of Metaverses

Christian Laue

Abstract With the development and spread of metaverses open to the public, criminology could face a new challenge. From the point of view of criminology, metaverses can be looked at from three different perspectives: First, there is the question whether metaverses open new dimensions to the already known Internet criminality. Looking at this more thoroughly, there is the danger of a quantitative increase of criminality in the Internet, but only low potential for the development of completely new forms of criminality. Second, virtual worlds can be regarded as separate societies for which the effects of deviant behaviour can be analysed by criminology, this resulting in severe conceptual and methodical problems. The findings of criminology in the real world can hardly be applied to the conditions of the virtual world. Finally, the use of virtual worlds could have feedback effects on the users in their real life. By imparting certain values and attitudes, the (excessive) occupation with virtual worlds could have effects on the behaviour in the real society. This question can so far hardly be answered and should be the object of further research.

1 Introduction

A Metaverse – a term usually attributed to Neal Stephenson’s novel “Snow Crash” – denotes a social virtual world. In this lecture, I will be looking at the “crime potential of Metaverses” in three different ways. The first question to ask is: To what extent do Metaverses open new dimensions of cyber crime? Do new opportunities for criminal activity result from Metaverses, whether quantitatively or even qualitatively? In this context, Metaverses must be considered and categorised as part of cyber crime. They

C. Laue (✉)

Institute of Criminology, University of Heidelberg, Heidelberg, Germany

e-mail: laue@krimi.uni-heidelberg.de

are thus regarded as part of existing cyber crime or as part of cyber crime that still needs to be developed.

Second, Metaverses can be seen as individual little societies in which deviating behaviour can lead to certain effects, which are comparable to the disturbances and irritations caused by criminality in real society. The question is whether deviating behaviour – which has to be defined as criminal – can lead to similar effects in Metaverses as crime does in real society. The consideration of social virtual worlds may even allow conclusions to be drawn about the causes and effects of crime in real society. Thus, Metaverses could be regarded as laboratories of real criminology: an attractive idea for every criminologist. In the following, I would like to call this the “criminology of Metaverses”.

While, in the first part of the lecture, Metaverses are viewed from the outside as separable parts of the Internet and, in the second part, from the inside as individual societies, it would only be logical to conclude by highlighting the links between the virtual and the real worlds. The issue that concerns us here is the knock-on effects that virtual worlds have on the real lives of users and how these can influence their behaviour in the real world. It is likely that virtual worlds convey certain attitudes and skills to their users as well as shortcomings that influence their real behaviour.

2 From the Outside: Metaverses as a New Challenge for Cyber Crime

Criminology, especially German criminology, has thus far paid little attention to cyber crime. When you look through the major German general literature on penal law, it is striking that the keyword “cyber crime” often does not feature at all (see Göppinger 2008). Only short papers can be found, such as the one by Eisenberg, who treats cyber crime as a manifestation of economic crime. For him, cyber crimes or multimedia crimes are “those criminally relevant acts that are committed using data networks (especially the Internet)” (Eisenberg 2005, Sect. 47 marginal no. 69).

There are hardly any other publications on cyber crime. This is astonishing since every year the Police Crime Statistics report highlights the rise in Internet-related crime. The Ministers of the Interior of the German federal states are convinced that the Internet offers great potential for crime [see, e.g., the Federal German Minister of the Interior, Wolfgang Schäuble (2007), during the opening of the BKA-Conference (German Federal Bureau of Investigations) “Tatort Internet” in 2007].

The “Polizeiliche Kriminalstatistik (PKS)” (German Police Crime Statistics) – usually taken as an initial guide to gain an overview of the extent and development of the overall number of crimes or types of offenses – has reported a separate category, “computer crime”, since 1987. This category comprises a number of criminal acts for which the use of a computer is required or is at least helpful to carry them out. The term “computer crime” is based on criminal law and does not report cyber crime as a separate category.

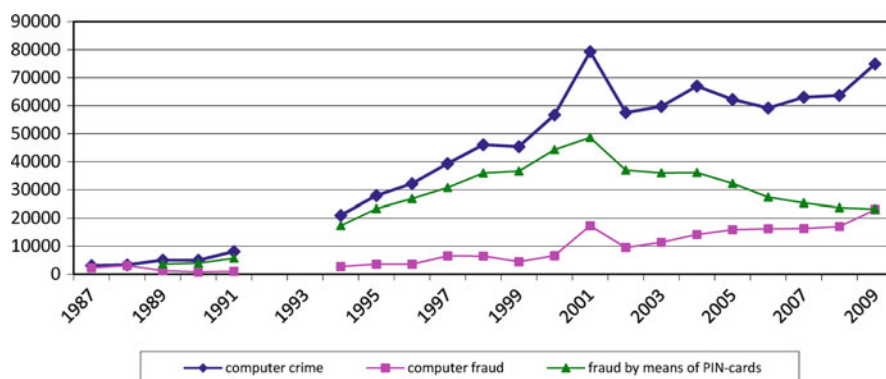


Fig. 1 Computer Crimes from 1987 to 2009. Source: BKA (German Federal Bureau of Investigation, ed.): Polizeiliche Kriminalstatistik 1987–2009

For our purposes, however, the PKS is of minor importance only, since the collective term “computer crime” includes hardly any cyber crimes, but rather fraud offences (such as computer fraud according to Sect. 263a StGB (German Criminal Code) or fraud by means of PIN cards obtained illegally).

Nevertheless, the PKS at least provides a rough overview of the development of cyber crime. In 2009, 74,911 computer offences were recorded in Germany, which is 1.2% of the total number of offences (6,054,330). In the first 15 years in which computer crimes have been recorded separately, the absolute figures of offences recorded have increased 26 times to almost 80,000 in 2001. Although the German reunification has to be taken into consideration, the rise is nevertheless constant, which is hardly surprising as, during these years, the computer has become indispensable in globalised society. It is much more amazing that there has been no further rise in computer crime from 2001 onwards, but rather stagnation. This is very remarkable, especially in the context described here, since the Internet has become extremely widespread during this period. In Europe, the number of Internet users has risen from 106 million at the end of 2000 to 385 million in 2008 (according to Internet World Stats 2009) (Fig. 1).

2.1 Types of Cyber Crime

Following David Wall (Wall 2001), four types of cyber crime in particular are identified internationally:

- “Cyber trespass”: Trespassing on and/or damaging another person’s computer, e.g. by “hacking” or sending viruses.
- “Cyber thefts/deception”: Theft of material and also immaterial resources through piracy as well as credit card fraud via the Internet. Now famous is

the so-called “scam” or advance fee fraud, where the scammers pretend to transfer vast sums of money from Third World Countries– first by ordinary mail, later – in extended version – by e-mail. This kind of fraud promises the receipt of a huge commission after acceptance of a large sum of money; the victim has, however, been persuaded to make advance payments. Since this kind of fraud originated in Nigeria in particular, and Nigeria has reacted by implementing its own penal law (Sect. 419 of the Nigerian Penal Code), it is also called the “419 scam”. This type of crime has increased significantly through the use of the Internet.

Another kind of Internet fraud – in a non-technical sense of the term – is “phishing”. Faked e-mails prompt the victim to reveal sensitive data, especially bank details, which the offenders can use to gain access to the victim’s fortune.

- (c) “Cyber pornography/obscenity”: The Internet provides various new ways of transmitting and selling pornography. It is estimated that 2–12% of all websites have pornographic content. Child pornography is especially problematic as the Internet is excellently suited to the cheap production, circulation and transmission of pornographic images of children. The market for child pornography has been significantly expanded by the Internet and is difficult to control. It may be assumed that the Internet has considerably promoted the worldwide sexual abuse of children, since the market for its distribution has become much bigger.
- (d) “Cyber violence”: This term comprises all forms of psychic damage or incitement to physical damage – known as Internet stalking and cyber bullying.

There is one form of cyber crime that can be subsumed under cyber aggression and to which special attention is given in Germany: content-related Internet crime. Especially due to the punishability of the “Auschwitzlüge” (Auschwitz Lie) according to Sect. 130 of the German Criminal Code – an element of a crime that only exists in a handful of countries – statements/comments are punishable in Germany which, in other countries, are covered by the freedom of opinion. This shows that cyber crime can really have regional references.

2.2 New Dimensions of Cyber Crime by Metaverses?

The situation outlined above raises the question: What new opportunities for criminal activity do Metaverses provide?

(a) Cyber trespass

The danger of cyber trespass is probably not increased any more through the participation in virtual worlds than it is through the general use of the Internet.

(b) Cyber theft/deception

There are probably various new opportunities for cyber theft and cyber deception in social virtual worlds like Second Life, where business is conducted using currencies

that can be changed into real money. According to Sect. 263 StGB, it is a punishable fraud if someone knowingly sells a virtual object that in fact does not correspond to the requirements agreed upon or assumed upon purchase. The Internet is an enormous temptation for dishonest traders, since the impression of anonymity and non-apprehendability is given by the ability to hide behind user names or avatars. In fact, the access requirements to the Internet in many cases allow people to log in with an invented identity.

The potential theft of virtual objects is much more difficult to judge from a legal point of view and is also a new kind of offence, which is only conceivable in a social virtual world. The aim of Second Life is that users buy objects, such as shoes, to adorn their avatar and create a unique external appearance. These objects must be paid for with Linden Dollars and are thus property of the buyer. Where there is property, there are also potential thieves. If one avatar takes the objects bought by another avatar, this is, however, not fraud in the sense of Sect. 242 StGB, since this element of an offence presupposes the removal of a movable object, i.e. a physical object. The shoes bought in Second Life are, however, not physical objects, but rather virtual objects, i.e. immaterial pixels. They can only be “taken away” by programme manipulations. Such behaviour would be criminally relevant as computer fraud/deception according to Sect. 263a StGB, assuming an unauthorised action on a computer programme – this would be the criminal relevance in the real world. In the virtual world, however, it would be theft, since one avatar takes away a thing from another avatar. We have to bear in mind that such an act – the virtual “theft” – is only possible in a virtual world in which the users can own property. In this respect, it is possible that Metaverses bring about new forms of criminal behaviour.

Cyber currencies in virtual worlds are only a quantitatively new dimension, although, supposedly, a very large one. Metaverses offering economic activity with a currency of its own that can be exchanged into real money are an invitation for money laundering. It is, however, questionable whether the economic system in Second Life will really be a central point of contact for money launderers. The Internet is already an ideal place for laundering illegal money (see Rederer 2000). Cyber currency, numerous business opportunities and an almost free choice of location already offer everything to disguise money laundering and to make it almost uncontrollable. Second Life could play a certain role in the circuits required for this because it offers all the ingredients for money laundering. However, it is not sufficient to be just an entrepreneur in Second Life to legalise illegal money without control. The large amount of publicity Second Life has experienced should lead to closer monitoring of any attempts to launder money there. Second Life could be another field of activity, but only one among many offered by the Internet. Metaverses are not generally expected to lead to a qualitatively new dimension of money laundering.

(c) Cyber pornography/obscenity

Social Metaverses offer new ways of distributing pornographic images. In 2007, Second Life ran into problems because individual users had designed avatars that

looked like children and these were presented in pornographic images, which is punishable according to Sect. 184b StGB. There is no restriction of punishability due to the fact that these images are only fictitious for, according to general opinion, the term child-pornographic publications according to Sect. 184b StGB includes fictitious images, too (Kusch 2000). The virtual child pornographic images with avatars as subjects and objects were presented extensively – especially in Germany – in the media and Second Life came under great deal of pressure.

It was also easy to buy real, i.e. non-fictitious child pornographic images by e-mail from Second Life users and to pay for these with Linden Dollars. Some of the members use the opportunities for business activity provided by Linden Lab to disseminate child pornographic images. This can be seen at least as a quantitative extension of the possibilities of the Internet.

The distribution of pornographic publications to minors, which is punishable according to Sect. 184 StGB, is also problematic. Second Life does not have any effective age controls, which means that minors can easily log in. It is thus relatively easy for them to consume the pornographic images offered by Second Life. However, the virtual worlds do not extend the possibilities already offered by the Internet on websites such as “www.youporn.com”, which have no effective age controls either.

To sum up, it can be said that social virtual worlds in particular present new ways of distributing pornography, especially with regard to the fictitious presentation of child pornography. This is, however, not a qualitatively new distribution channel. Instead, Second Life, for example, offers an additional distribution channel via the Internet. Indeed, Second Life is not primarily a pornographic site; the main focus is still on other content. Sexuality and pornography are just part of a very large spectrum of possible content in virtual worlds. There is, however, a danger that pornographic distribution possibilities are concealed within the Second Life world where, on the one hand, potentially many users can be reached and where, on the other hand, the investigation authorities have very little control. The operators of virtual worlds should make it their mission to reduce such misuse. Very often, the police’s hands are tied in this respect (Report Mainz (ARD) broadcast of 7 May 2007).

(d) Cyber violence

For some people, the Internet has become an important social space. It not only provides information, knowledge and entertainment, but also the possibility to make social contacts. It is reported that the social contacts of some people are even reduced exclusively to the Internet. It is therefore not surprising that this development also leads to aggression and social violence.

The fate of the 13-year-old Megan Meier, who committed suicide in October 2006 after having been abandoned by her assumed, but fictitious Internet love, became well-known all over the world. This fictitious Internet character called “Josh Evans” had been created by a former schoolmate and her mother and neighbour of the victim’s family in the Internet chat room “MySpace”, and succeeded in charming Megan completely. In order to humiliate her, Josh one day

finished the relationship with nasty insults and exposed her on the Internet. Megan was unable to cope with this and hung herself that afternoon. In November 2008, the then 49-year-old mother of the schoolmate was sentenced for computer fraud by an American Federal Court because she had logged herself in at “MySpace” with a false name. Meanwhile, Missouri has passed new legislation concerning cyber bullying, which sets an example for other legal systems.

The fact that this case did not happen in a Metaverse, but in the well-known and widespread “MySpace” shows that this kind of bullying is not reduced to virtual worlds, but was already possible in the existing Internet. It is precisely in this respect, however, that a social virtual world such as Second Life opens up many possibilities. The “ingredients” for such bullying all exist in Second Life: the establishment of social contacts among virtual characters is the declared aim of Second Life. It seems clear that the exploitation of the difference in authority – as in the case of Megan Meier: a grown-up offender and a minor victim – is obvious and even encouraged. But this is a general danger of the Internet and its possibilities to make, but also to abuse social contacts.

It is worth mentioning two similar cases from Germany here: On March 30, 2009, the so-called “Chat room Murderer” Christian G. was sentenced to life imprisonment. He had met women via the Internet and then met up with them in the real world, causing the death of two of these women. At first glance, it seems doubtful that these offences are really caused by the Internet. However, when you read that the accused had virtually no social contacts in real life and that he was only able to make contacts by creating a second – virtual – existence, the opportunity to make social contacts via the Internet is perhaps not a sufficient condition for the offence, but is a necessary one.

This becomes clearer when you consider the famous case of the “cannibal of Rotenburg”, Armin Meiwes. In February 2001, he killed and ate a man he had met via the Internet and who had given his consent to being killed and mutilated. In this case, it is difficult to imagine that the offender and consenting victim would ever have met outside the Internet. Here too, the Internet seems to have been a necessary condition for the offence. There is some controversy as to whether it makes sense to count such a case as a cyber crime. It is characteristic in each case that the offenders would hardly have come into contact with their later victims without the help of the Internet. In the case of the “cannibal”, the Internet offered the extremely low probability of meeting a consenting victim. The range of potential social contacts was significantly widened by the Internet. In the case of the “chat room murderer”, he was able to construct a virtual identity, which deviated from his real identity, and thus make himself much more attractive to real contacts.

Metaverses also offer the opportunity to construct virtual identities – this is even their objective to a large extent. However, Metaverses are not a new dimension of the Internet for committing crimes since – as shown by the two cases above – these possibilities already exist on the Internet.

Social virtual worlds, however, pose another challenge for a criminological discussion. On the one hand, there is the criminologically relevant behaviour of

the users in the virtual world, and on the other hand, possible repercussions between the use of a virtual world and behaviour in the real world.

3 Metaverses from the Inside: Criminological Research

Some virtual worlds, especially Second Life, regard themselves as a separate society offering their users an individual social field of activity that should be as similar as possible to real society. Users can make social contacts, they can invest, found enterprises, have economic success, they can be creative or – more passively – enjoy their spare time and travel or just use artistic or entertainment programmes.

In such an environment, there is always the possibility that individuals show deviant behaviour and thus damage other individual avatars/users or the virtual community as a whole. This socially damaging behaviour could be described as criminal.

Social virtual worlds are seemingly opening up unforeseen possibilities for criminological research: Would it not be possible to conduct criminological research e.g. in Second Life – a relatively manageable area compared to the real world – and then draw conclusions on criminological relationships in the real world? Second Life as a kind of a social laboratory, which – on human rights grounds – would not be possible in the real world; a field of experiments just to answer criminological questions?

If Second Life is an image of real society in virtual space, the same mechanisms and social laws must surely apply as in real life. Criminologists could then conduct their research in a manageable framework and, e.g., empirically verify the well-known theories on the origins of crime in the laboratory situation of virtual space. This is a tempting idea. A closer look at this, however, reveals three counter-arguments.

3.1 The Problem of Measuring Crime in Metaverses

It is probably very difficult to measure the number of crimes in virtual worlds. In the real world, crime statistics give us a rough idea of the extent and development of crimes – despite all the reservations against them. These statistics form an indispensable basis for numerous research projects and they do not exist in the virtual world. It would, of course, be possible to interview the users, and this would correspond to the interviews of so-called “dark field” research. These would have to be modified – the intensity of the use of the virtual world would, e.g., have to be measured since Second Life users are only part-time users, whereas citizens of the real world are always citizens. Details on offenders or victims would have to be put into relation to the extent and use of the virtual world. This obstacle, however, could be overcome.

3.2 The Problem of Crime Definition in Metaverses

What does crime in the virtual world really mean? This question is much more difficult to answer. The question of how to define a crime adequately is a problem not satisfactorily solved in criminology and is one that might perhaps never be solved. There is a formal notion of “crime” in criminology: crime is a behaviour defined as criminal by the legal system. Judging crime in the virtual world is compounded by even more problems, since such a formal evaluation is impossible. Second Life itself deliberately avoids regulating the behaviour of its avatars. Thus, the only option would be to recourse to the national or international legal systems of the real world. This would inevitably result in different assessments/evaluations, since e.g. the “Auschwitz Lie” of Sect. 130d StGB – a very important offence concerning the German legal assessment of the Internet – would hardly have a counterpart in other countries and would thus be of no relevance for other researchers. The international comparability of possible results would be very limited.

There would only be a small number of offences that could be examined sensibly. As already mentioned, a theft in the virtual world – by far the most frequently committed offence in the real world – would be computer fraud in the real world. Finally, most of the deviant behaviour which, in the real world, is an element of a crime of the core criminal law – theft, robbery, damage to property, arson, rape, bodily injury or homicide – can only be reduced to a computer offence: computer fraud, modification of data, or computer sabotage.

3.3 The Problem of Crime Effects in Metaverses

Finally, we must take a look at the persons in question, or rather the avatars. It is questionable whether deviant behaviour in virtual worlds can really lead to such social damage as in the real world. The possibilities of victimisation are already significantly reduced: a homicide or murder offence is hardly conceivable in Metaverses, since it is a characteristic of a virtual world that every participant has a number of or even an unlimited number of lives. If an avatar loses its life – and this happens very often in many online games – it cannot really be regarded as the victim; this is at least not remotely comparable to victimisation in the real world. Thus, potential crimes in virtual worlds lose much of their threatening effect.

There could be effects in the area of fraud or virtual theft. The economic activity promoted by Second Life could really be brought to a standstill if acts of fraud were carried out on a massive scale, because honest entrepreneurs would lose interest. An effective control would be necessary here, and it could be interesting for criminological research to observe how order could be brought to a world with a self-selected lack of rules.

This, however, only touches on a small portion of crime; the types of crimes that are particularly important to the real general public hardly play a role in virtual worlds.

You also encounter problems when you consider the offenders. When an avatar is insulted, who is the offender? Who must be punished – in as far as it is hoped that punishment will have any effect at all? And, if the avatar is punished – there might be the possibility of sending him to a virtual prison – who would actually be affected by the punishment? Ultimately, the user behind the avatar is responsible and only he can feel the punishment. This means there is no punishment for the behaviour of the avatar but only for the behaviour of the person sitting in front of the computer.

Thus, the view of the virtual world as an autonomous society is, in most cases, inadequate. Only in cases where real social acts are directly transferred to the virtual world – especially with regard to commerce in Second Life – can real social findings be transferred to the virtual world.

4 Repercussions of Metaverses on Reality

The third interesting problem for criminology concerns how the use of virtual worlds affects the behaviour of users in the real world.

I will only touch on this briefly here, since the following lectures will go into more detail. Concerning the question of the effects of Internet use, a possible increase in the willingness to use violence – after numerous relevant cases – is at the focal point of criminology and also criminal policy. A number of violent acts at American and European schools seem to have been inspired by computer games; it is, however, doubtful whether these are to be attributed to Metaverses. This will certainly become clearer in the following lectures.

Less obvious is the possibility that Metaverses which, in many cases, are a monopolising social counter-world, are able to create and care for values and attitudes among their users. There are reports about people spending more time in virtual worlds and on the Internet than in real society whose social contacts are concentrated on the Internet, in short, people who spend more time with avatars than with human beings. These replacement worlds could tend to create their own values and norms. If these values and norms are contrary to the values and norms of real society, subcultures emerge. And if these social worlds have an influence on their users, it may be possible that they will take the values and norms of the virtual world and apply them to the real world. This and the resulting conflict between the norms and values of virtual society and those of real society could influence the behaviour of the users and, probably, also increase crime. So far, little research has been conducted in this field, although it could prove to be worthwhile.

5 Summary

In summary: The existence of Metaverses does not call for new criminology. A qualitatively new dimension of crime is possible only in marginal areas; in most cases, Metaverses simply provide new fields of investigation for the now well-known cyber crimes. There remains, however, inadequate research in this field in Germany.

References

- Bundeskriminalamt (2009) Polizeiliche Kriminalstatistik Bundesrepublik Deutschland. Berichtsjahr 2008. Bundeskriminalamt Wiesbaden
- Eisenberg U (2005) Kriminologie. Beck, München
- Göppinger H (2008) Kriminologie. Beck, München
- Internet World Stats (2009) <http://www.internetworldstats.com/stats.htm>. Accessed 30 Jun 2011
- Kusch R (2000) Aus der Rechtsprechung des BGH zum Strafverfahrensrecht. Neue Zeitschrift für Strafrecht Rechtsprechungsreport:289–320
- Rederer E (2000) Geldwäsche mit Cybermoney. Oder: Wie tradierte Bekämpfungsstrategien wertlos werden. Kriminalistik. Unabhängige Z kriminalistische Wissenschaft Prax 54:261–269
- Report Mainz ARD (2007) “Second Life.” Tummelplatz für Kinderpornografie, 7 May 2007. <http://de.youtube.com/watch?v=Wk8uNWF77gg>. Accessed 16 Mar 2010
- Schäuble W (2007) Tatort Internet – eine globale Herausforderung für die Innere Sicherheit. Rede zu Beginn der BKA-Konferenz. http://www.bmi.bund.de/cln_165/SharedDocs/Reden/DE/2007/11/bm_bka_herbsttagung.html. Accessed 16 Mar 2010
- Wall DS (2001) Cybercrimes and the Internet. In: Wall DS (ed) Crime and the Internet. Routledge, London



<http://www.springer.com/978-3-642-20822-5>

Virtual Worlds and Criminality

Cornelius, K.; Hermann, D. (Eds.)

2011, IX, 124 p., Hardcover

ISBN: 978-3-642-20822-5