

**Subject:                        Prevention of deviant behaviour around the internet**

---

## **1    Problemdescription / starting situation**

Since the nineties of last century the internet has made an enormous development from the communication media of elitist, often scientific circles to a mass media with nearly one thousand million users. In addition to the mainly passive research of information, the world wide web (WWW) offers a multiplicity of possibilities - from electronic data exchange via eMail, by chatrooms up to remote control of computers. Today's information society is not imaginable any more without the internet. Many households are equipped with a computer and internet access and even primary school pupils are accustomed to its functionalities and are "at home" in the internet.

Yet sooner or later every useful achievement is abused for criminal purposes. Not only communication with all parts of the world is possible via internet but users have to face more and more criminal contents and methods. The spectrum stretches from all kind of fraud to prohibited right-wing-extremist or child pornographic contents.

The internet is the communication media of the future. Terms, such as eBanking, eLearning, eCommerce and eGovernment are not only vogue words but represent new, permanently developing forms of interaction in multiple fields of life. In a way it is the net of social future. Therefore a society must not accept that single groups of the population are uncoupled from the development, whether by lacking know-how or by fear of factual or supposed dangers of the new technologies.

As a result of the evaluation of certain studies and projects/initiatives on the subject of "general development", "dangers/criminality", "technique", as well as "media competence" in connection with online-media the situation can be sketched as follows:

Due to the requirements of business partners and of public administration as well as of consumer expectations, in Germany nearly all companies will use the internet for their business before long.

- The number of private internet users will continue to increase with a decreasing speed. The internet will be used complementarily to classic media. Especially people of a lower level of formal education as well as the over-fifty-years-old people will be significantly underrepresented and will be excluded increasingly from the progress of the society ("digital divide").
- The development of children and adolescents will intensively be influenced by the information and media society. The same way as in the "off-line-world", their media use will decisively be formed by peer structures and school. Family influences do nearly not matter, not least because of the parents lacking media competence.

---

<sup>1</sup> Literature evaluation of the project: prevention of criminality around the internet; 2005-06-14 (intern) Literaturauswertung Projekt: Prävention von Kriminalität rund um das Internet; 2005-06-14 (intern)

- The convergency of media contents, use of media and media equipment will increase. Especially the rate of mobile units and accesses will rise. The development of the information society which is formed by the providers makes increasingly high demands on the users. They do not make use of a large number of the functionalities of modern equipment nor do they understand them or have command of them.
- Criminality within the internet registered by the police shows an increasing tendency with a considerable expected number of unknown cases. In addition to attacks against the internet itself and against offered services in a broad sense (the internet as object of the crime), the internet can be used to commit nearly every delict (the internet as means of the crime). The economic loss runs into thousands of millions.
- Aspects of adolescent media protection are considered only insufficiently in the internet, even by profiled providers. At present there are no effective technical protection precautions, which consider protection of children and adolescents against illegal contents or against contents influencing their development, as well as the right of free statement and free access to information.
- Present structures of administration, investigation, justice and jurisdiction are not appropriate to encounter efficiently the risks arising with the development of the information society.
- There is no distinct conscienceness of injustice for internet delinquency. Certain conditioned obstructions, which influence the behaviour in face-to-face situations seem to be partly suspended within the virtual (anonymus) world. Basic effective norms and rules of the offline world have not yet been transferred sufficiently into the online world.
- Many internet phenomens evoke their own security and protection requirements and cannot be directed only nationally, especially because of the net's globality. In addition to this, many ways of acting are normatively not regulated homogenously and definitively. This is why it seems to be indicated to rather speak of "delinquency" than of "criminality".
- The complexity of IT-systems is increasingly overcharging many users. The expectation of developping confidence in the technique will hardly be fulfilled, considering security problems and dangers arising in increasingly short periods. The link between offer and demand has already gone lost here.
- The current information technolgy is considerably susceptible for attacks and misuse because of the chosen technical solutions. Safety of the infra-structure will either be improved successfully or this infra-structure can and may not be used anymore for certain purposes.
- In spite of the findings about risk potentials and factors which initiate or encourage damage as well as precautions, the risk conscienceness of many potential victims and sufferers is still developped only rudimentarily.
- Up to now the main focus of approaches to combat internet criminality is in the technical field. But more and more the fact occurs that developments which are considered to be final for internet security today, cease to be effective already tomorrow. There is a permanent race between the safety industry and increasingly professional offenders.
- Man remains the most weak chain-link: whether mistake, misoperation, calculated attacks, loss of mobile equipment including data or lacking conscienceness of injustice,

most security incidents are caused by human beings. In addition to this, even technically perfectly secured systems cannot prevent the committing of criminal offences via internet such as fraud or spread of illegal contents.

- Media competence does not only mean the ability to handle computer and internet correctly but to handle their contents sensibly, to estimate and to value them according to their quality and meaning as well as to know risk potentials and measures of protection and to utilize them. At the present here still are important deficits.
- Existing offers for the procurement of media competence do not take the preferences of use of different population groups into consideration, but are often designed according to the providers' view and their ideas about the way of use.
- Up to now there is not paid enough attention to people and their behaviour as crime forming factors in connection with internet criminality. There is a lack of research results about factors which influence the individual's behaviour in virtual environments, and by consequence there are also no persistent conceptions of prevention in this area as well as no general conception for the development /supply of media competence as a basic ability of the modern information society.

Taking all this into account and considering the development of the IT-technique and of the IT-safety as basic conditions, it seems to be essential to put the individual and his behaviour in the center of the study as important crime forming factors for delinquency around the internet. It is important to view questions of the development of conscienceness of injustice and risk in the virtual world as well as to look at an efficient, target group oriented supply of complete media competence in dealing with the internet and further online media. On this basis a future oriented, systematic and complete conception of prevention can be elaborated. A concentration and coordination of prevention measures of various actors basing upon this, might increase the effectivity and the efficiency of prevention and at the same time be conducive for a better acceptance of the internet.

## **2 Activities / Contributions of DFK**

### **2.1 Expert-Workshop on 2006 February 14<sup>th</sup> and 15<sup>th</sup> in Bonn**

(organised by DFK)

#### **Programme:**

- New media, new chances, new risks and new delinquency within the information society (Prof. Dr. Jo Groebel, Institute for the Media, Dortmund)
- The relevance of the internet to the life of juveniles: new aspects of Youth culture (Thomas Rathgeb, Media Education Research Network Southwest, Stuttgart)
- Basic conflicts and controversies by dealing with the „intellectual property“ within the knowledge- and information society (Dr. Andreas Degkwitz, University of Technology Cottbus)
- Prevention and prosecution of „digital piracy“ by the view of commercial authors and providers (Jan D. Scharringhausen, German Federation against Copyright Theft, Hamburg)
- Digital mentalities: The change of strategy in dealing with „Crackers“ (Hergen Wöbken, University of Witten-Herdecke / Institute for Strategy Development)

- Phenomenons of e-fraud (especially within e-commerce and e-auctions) and prevention potentialities (Oliver Stutz, data protection north Ltd. / Initiative D21)
- Limits of technology and the relevance of psychological factors for the development of conceptions of e-fraud-prevention (Ivan Martinovic, University of Technology Kaiserslautern)
- Different approaches to fraud prevention in the e-commerce – development of trust by internal reputation systems delimited from external sanction systems (Stefan Wehrli, Swiss Federal Institute of Technology, Zurich)
- Cyber – Stalking – blackmailing and psychologic violence at internet-communication (Dr. Jens Hoffmann, University of Technology Darmstadt)
- The effects of internet pornography  
(Dr. med. Andreas Hill, University Medical Center Hamburg-Eppendorf / Department of Sexual Research and Forensic Psychiatry)
- Suicide forums in the internet: Risk or benefit for prevention?  
(Dr. Christiane Eichenberg, University of Cologne)
- Approaches to increase the risk awareness of Onliners regarding viruses, worms, trojans, hoaxes etc. (Frank W. Felzmann, Federal Office for Information Security)
- New ways of criminological dark field research and prevention? Procedures, experiences and problems with electronic baits (>Honeypots<) (Dr. Maximilian Dornseif, University of Mannheim)
- Industrial espionage – internal prevention in the system of commerce (Jörg Meyer, KPMG Deutsche Treuhand-Gesellschaft AG Wirtschaftsprüfungsgesellschaft)
- Presentation of existing internet specific initiatives of media competence and prevention in Europe  
(Dr. Gernot Gehrke, European Centre for Media Competence, Marl)  
(Mrs. Ann-Katrin Agebäck, Swedish Media Council, Stockholm)  
(Mrs. Leena Karjalainen, „Save the Children Finland“, Helsinki)  
(Mrs. Jarmila Knight, Educational Institute for Child Protection, Prag)

Most of all presentations are documented in an workshop-reader “Internet-Devianz” in German language.

## **2.2 EUCPN-Seminar 2007 June 1<sup>st</sup> in Wiesbaden**

(organised by Federal Ministry of Interior BMI)

### **Programme:**

- On the relevance of the internet for young people’s lives – new aspects of youth culture” (Mr. Thomas Rathgeb, Medienpädagogischer Forschungsverbund Südwest [media education science institute], Stuttgart)
- New media, new opportunities, new risks and new types of delinquency in the information society” (Prof. Dr. Jo Groebel, Deutsches Digital Institut [German Digital Institute], Berlin)
- On the effects of pornography in the internet” (Dr. med. Andreas Hill, Universitätsklinikum Hamburg-Eppendorf / Institut für Sexualforschung und Forensische

Psychiatrie [University Hospital Hamburg-Eppendorf/Institute for research into sexual behaviour and forensic psychiatry])

- Presentation No. 4: Swedish prevention approach (Ms. Ann Katrin Agebäck, Director of the Swedish Media Council [Medierådet])
- Presentation No. 5: Approach from Finland (Ms. Mari Laiho, Project Officer, Save the Children Finland)
- Presentation No. 6: Approach by German police authorities (Mr. Reinhold Hepp, KOR, Polizeiliche Kriminalprävention der Länder und des Bundes ProPK [Programme for police crime prevention on the Laender and Federal levels, Criminal Police Authority of the State of Baden-Württemberg])

### **2.3 DFK Working Group**

**In May 2007 was decided to implement a multidisciplinary Working Group. Preparations are therefor going on.**

#### **Targets in kind:**

- The phenomenology of (crime-)dangers which result from the use of online media around the internet and factors which are favourable to these are gathered and rated.
- Factors which influence human behaviour in the virtual area as well as at the intersection with the real world are examined scientifically, especially with view at the questions of awareness of injustice, of risk as well as at the reaction on identified danger potentials.
- Requirements for the necessary media competence while using online media are defined with consideration of existing risks.
- Target group specific models for supply of necessary media competence as well as for support of the awareness of injustice and risk in the virtual room are developed and taken up in a future oriented, systematic and complete conception of prevention with advice for realization.

A project plan will be published as soon as possible.