CYBERCRIME
DEFINITIONAL CHALLENGES AND CRIMINOLOGICAL PARTICULARITIES

by

ALEŠ ZAVRŠNIK*

The very concept of cybercrime is still a very vague notion. There are different types of "lenses" used to observe cybercrime and consequently many contradictory "facts" about its scope. Article shows different forms of what we call "cybercrime" and the variety of assessment of its dangerousness. It presents origins of cybercrime regulation and current disputes on the Council of Europe's allegedly impartial and independent legal solutions. In spite of the definitional heterogeneity it defines novelties in the notion of cybercrime and more or less accepted legal definitions and taxonomy. In order to escape one-sided estimates of the real danger posed by cybercrime, article does not rely solely upon legal definitions of illicit behaviour in cyberspace. Additionally, the phenomenon of cybercrime is examined through sociological reflections of cyberspace and cyber (contra-) culture. These are important for the understanding of the criminological/victimological pair: offenders and a 'hacker culture' on one hand, and victims and victimological characteristics on the other. After analyzing a social construction of hackers, the article outlines the ideological struggle for primacy over cyberspace: a struggle between contra-cultural values, interwoven in the very creation of cyberspace and the values of post-modern digital capitalism; a struggle for the primacy fought between a computer "underground" on the one and the security and cultural industry on the other hand.

* Aleš Završnik, LL.D., researcher, Institute of Criminology at the Faculty of Law, Ljubljana, Slovenia. Poljanski nasip 2, SI-1000 Ljubljana, Slovenia. E-mail: ales.zavrsnik@pf.uni-lj.si.

KEYWORDS

Cybercrime, criminology, victimology, offenders, victims, structural violence, cybercrime regulation, computer integrity crime, computer-related crime, computer content crime

INTRODUCTION

DUBIOUS "FACTS" ABOUT CYBERCRIME [1]

The very concept of cybercrime as a side-effect of the "information revolution" and its most famous "product" – the internet – is still a very vague notion. The vast literature about the nature of cybercrime can be divided into a number of discourses. Wall,[1] for instance, identifies (1) the legislative discourse about cybercrime which attempts to define the rules that set boundaries for (un)acceptable behaviour, (2) the academic discourse that seeks to understand the phenomenon through computer science, information management, economics, and from the perspective of the socio-legal and criminological disciplines (3) the expert knowledge that explores and seeks to understand trends in cybercrimes in order to provide explanations and inform solutions and (4) the popular/layperson's discourse that reflects a "common sense-based" understanding of crime. The problem we face today is that all these different discourses, approaches or narratives are incoherent, and their claims to knowledge often contradictory. Do acts labelled as "cybercrimes" really represent a "clear and present danger" to our "information societies"[2] which in turn requires the machinery of the criminal justice system to be set in motion?

According to a recent report from the Council of Europe,[3] current trends in the fields of information and network security are far from encouraging. (1) Information societies worldwide are increasingly dependent on information and communication technologies and the growth of cybercrimes

[1] Wall 2007: 12.

[2] The European Union emphasizes its determination to evolve in the so called »information society« in the Lisbon Strategy (2000-2010), (former) eEurope 2005 Action Plan and the i2010 Strategy (2005-2010). Among the primary concerns expressed in all of the above-mentioned documents are network and information security and fight against cybercrime.

[3] Octopus Interface 2007 »Cooperation against Cybercrime«, 11-12 June 2007, Palais de l'Europe, Strasbourg, France.
URL: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_technical_cooperation/CYBER/Octopus_if_2007.asp#TopOfPage, 14.12.2007.

renders societies highly vulnerable. (2) Malware (malicious codes and software, including viruses, worms, Trojan horses, spyware, bots and botnets) is evolving and spreading rapidly, and is being used among other things to commit 'denial of service attacks',[4] identity thefts, frauds, money laundering etc. (3) Spam now represents the vast majority of email traffic and is not only a nuisance but is increasingly a carrier of malware: in addition, spam messages are also appearing in new technologies (on mobile phones as SMSishing or internet phones as Vishing). (4) Botnets[5] are one of the central tools of organized cyber crime used for DoS attacks, identity thefts, phishing,[6] as well as for the placing of adware and spyware etc. (5) An underground service economy is developing (botnets are being leased to organised criminal groups). (6) The threats are changing: the mass, multi-purpose and global attacks by viruses, worms or spams which attracted so much public attention are being replaced by more targeted and smaller attacks on specific users, groups or organizations, seemingly with the aim of avoiding attention and pursuing instead a concerted economic purpose. (7) Online virtual payment systems are becoming a major concern in the USA. (8) The internet is misused for the sexual exploitation and abuse of children and human trafficking (child pornography in particular has attracted an increasing commercial interest). (9) The risk of cyber-attacks against the critical information infrastructure (cyber-terrorism and cyber-war) is perceived to be on the increase.[7] (10) The use of P-2-P networks[8] supposedly enables widespread copyright infringements. (11) The technologies and techniques used

[4] Denial of Service attack (DoS attack), also called Distributed Denial of Service attack (DDoS attack).

[5] *Botnet* is a network of "hijacked" ("zombie") computers. It comprises lists of the internet protocol addresses of "zombies" that have been infected by remote administration tools and which can subsequently be controlled remotely. ('Bot' is an abbreviation of robot.) According to moderate estimates today at least a million computers are "zombies". Reimer 2007.

[6] *Phishing* is a process of catching of personal data (thus the neologism coined from *fishing*); for instance an e-mail (phish) or counterfeited webpage demands that a user discloses her password or export a digital signature etc.

[7] Cyber terrorism denotes attacks on so called "critical information infrastructure", compounded from gas, electricity and water supply enterprises, telecommunication companies etc. According to some estimates the vast majority (95%) of such companies in the USA and EU do not invest in appropriate protection from cyber attacks, although there were more than 180.00 attacks on that kind of users in the first half of 2002 and the increase rate of attacks is 60 percent a year; in addition, reported security incidents are thought represent only 10 percent of all attacks. Departing from the presumption that only 20 percent of cyber attacks are being reported, FBI estimates that attacks on private infrastructure in USA cause 10 milliard US dollars in damage. (Ashenden 2002; Lewis 2006).

to commit cybercrime are developing rapidly and, in addition, next-generation-networks (NGN) (technologies including internet telephony – Voice-over-Internet Protocol, internet television – IP TV, Video on Demand – VoD) will pose new challenges to law enforcement. Finally, estimates of the material damage caused by cybercrime put the cost at around 50 milliard dollars a year.[9]

The trends listed above and the diverse phenomenology of cybercrime show, firstly, that the identification and analysis of cyber threats is still an arduous task. There are different forms of what we call "cybercrime": some forms "only" use computers and networks as a means for committing conventional crime, while others focus primarily on computers, networks and data; some are computer crimes (the so-called first generation of cybercrime), others involve hacking (second generation) and some automated forms of cybercrime (third generation).[10]

Secondly, the list shows that the evaluation of the danger of cybercrime is self-contradictory. According to the report from the Council of Europe discussed above, the work of an organization that is undoubtedly one of the most important forums for the protection of human rights, we should be afraid for the threat the problems in this list pose to individuals; actually, very afraid. If we accepted the report in its entirety the only possible conclusion is that cybercrime clearly and seriously threatens our information societies. But, many criminologists are warning us not to draw such conclusions.[11] They claim that this anxiety is being provoked, quite intentionally, by certain parties pursuing their economic interests and by others trying to make their voice heard in the process of reallocating public funds. For instance, security software manufacturers are without question extremely interested in alarming the public and raising the question of cyber security closer to the top of society's agenda. Yet the case of spam clearly shows us that the danger of cybercrime can be exaggerated. At the beginning of 2007

[8] P-2-P (peer to peer) networks are networks of equivalent users and enable file sharing. There are B2B (business to business) and B2C (business to consumer) variations of technology.

[9] For instance, only one of the most notorious worms called *"I Love You"* is estimated to have caused 11 milliard dollars in damage. Other attacks on *Yahoo!*, the auction website *eBay* and the e-store *E*Trade* cost 1,2 milliard dollars in damage. (Kumar Katyal 2001: 1003).

[10] More about automation of offender-victim engagement in Wall 2007: 130–156.

[11] Levi 2001; Wall 2002; Wall 2007.

there were estimates that spam represented 80 percent of e-mail traffic in 2005, 95 percent in 2006 and that the system will reach its capacity in 2007.[12] This disaster has (thankfully) not occurred, but "anxiety-provokers" will quickly add that has only been averted by the system's ability to adapt; should this fail, we shall be in trouble. Perhaps the pessimists' claim has some weight, but the performance data supplied by sources in criminal justice systems across Europe (i.e. statistics from police forces, prosecution services and criminal courts) gives opposing evidence that the numbers of reported crimes, and of prosecuted and judicial cases simply are not growing as quickly as some claim and fear; and moreover that they do not justify a verdict as dire as that which the Council of Europe's report would have us reach. On the contrary, the numbers themselves are extremely low and contrast sharply with the non-numerical "situation analysis" the report offers.

In order to escape one-sided estimates of the real danger posed by cybercrime, this paper does not rely solely upon legal definitions of illicit behaviour in cyberspace. Instead, we shall be examining the problem through sociological reflections of cyberspace and cyber (contra-) culture. These are important for if we are to understand the criminological/victimological pair: offenders and a 'hacker culture' on one hand, and victims and victimological characteristics on the other. This paper illustrates more specific characteristics of cybercrime victimization and cyber deviants, hackers or "console cowboys". After analyzing a social construction of hackers', the paper outlines the ideological struggle for primacy over cyberspace: a struggle between contra-cultural values, interwoven in the very creation of cyberspace and the values of post-modern digital capitalism; a struggle for the primacy fought between a computer "underground" on the one and the security and cultural industry on the other hand.

DEFINING CYBERCRIME [2]

The answer to the question "how should we react to online deviant behaviour?" clearly depends on how we define such behaviour, and on how we define cybercrime. The (similar) word cyberspace was coined by William

[12] Le Monde, 11th May 2007, URL: http://www.lemonde.fr/, 11.5.2007. Look also Rowan, D., Britain is flooding the world with spam. Po URL: http://www.timesonline.co.uk, 27.4.2006.

Gibson in his famous cyberpunk novel Neuromancer in 1984. The author[13] designed an imaginary world and language to describe it already a decade before the "information revolution" and expansion of the internet. The understanding of the fundamental ontological concepts of cyberspace that arose from the cyberpunk movement in the eighties would seem to be indispensable to understanding properly (at least some forms of) cybercrime. The 'cyberpunk' is characterized by a belief in using technology to support and cultivate individualism, and allow for the possibility of a "self-determined human being". The term bespeaks an allegiance to and an insistence upon the idea of self-creation, through the independent selection of identities no longer determined by tradition. These attributes of cyberpunk are all typically post-modernist characteristics, attributes which migrated in the nineties well beyond science-fiction literature as the notion of cyber culture became a part of daily life.

The roots of cyber culture are to be found in the revolutionary, counter-cultural period which characterised the 1960s. This was an era largely defined by a struggle against the scientific – or over-empirical – comprehension of reality and technology. A transformation took place later in the 1980s when counter-culture united (paradoxically and ironically, as it turned out) with forms of technology that seemed to offer some means of escaping from extensive societal controls. In these terms, cyber culture encompasses an aspiration towards the emancipation of the individual that was gradually taken over and restrained by large trans-national technological systems. Today, appreciating these roots of cyberspace is important if cybercrime is to be understood, especially the villified hacker culture: for that culture, as we shall see, was primarily based on the principle of a gift economy, involving open access and the free sharing of knowledge. Before taking this side of the discussion further, let us turn to the legal discourse on cybercrime that I will try to question.

[13] Notions belonging to the counter-cultural cyberpunk context, such as clone, cyborg, simulacra, simulacrum, matrix, hyperreal etc., were generated in artistic works and genres, mostly literary and cinematic; it was only later that they acquired a social (scientific) reflection.

ORIGINS OF CYBERCRIME REGULATION [2.1]

The Worldwide interoperability of information systems and the cross-border nature of cybercrime developed in consequence are the main reasons that the intensive drive to formulate substantial and procedural criminal rules against cybercrime manifested itself at an international level. The exhaustive formulation of the criminal "fight" against "computer crime" (as it was then called) began under the auspices of the Organisation for Economic Co-operation and Development (OECD). Its ad hoc commission investigated the possibilities for the international harmonization of criminal laws in the fight against economic crime related to computers. International efforts continued in the United Nations when a manual on the prevention and control of computer-related crime was adopted at the Eighth United Nations' Congress on the Prevention of Crime and the Treatment of Offenders in Havana in 1990. The manual describes the phenomenon of computer crime and contains some of the first substantive and procedural criminal law provisions.[14] The importance of cybercrime was further stressed at the G-8 Conference on Cybercrime in 2000. But the contemporary and very influential criminal law provisions against cybercrime were not adopted until 2001 with the Council of Europe's Convention on Cybercrime.

The Convention on Cybercrime is the first comprehensive international agreement on combating "high-tech" crime by means of criminal law.[15] Since the adoption of the convention, the Council of Europe has taken the initiative in combating cybercrime through the law: when for instance the Convention Committee on Cybercrime (T-CY) was formed, the subject became a part of the Octopus Programme that organizes annual international conferences dedicated to problems of cybercrime, among other ongoing ini-

[14] The United Nations Manual on the Prevention and Control of Computer-Related Crime defines the following computer-related crimes: (1) fraud by computer manipulation, (2) computer forgery, (3) damage to or modifications of computer data or programs, (4) unauthorized access to computer systems and service and (5) unauthorized reproduction of legally protected computer programs. (*United Nations Manual on the Prevention and Control of Computer-Related Crime,* 4 U. N. Doc. ST/ESA/SER.M/43-44, U. N. Sales No. E.94.IV.5.)

[15] The *Convention on Cybercrime* distinguishes the following groups of cybercrime: (1) offences against the confidentiality, integrity and availability of computer data and systems (i.e. illegal access, illegal interception, data interference, system interference, misuse of devices), (2) computer-related offences (eg. computer-related forgery and computer-related fraud), (3) content-related offences (eg. offences related to child pornography), (4) offences related to infringements of copyright and related rights. The convention entered into force on July 1 2004.

tiatives.[16] But the Council of Europe's legal solutions concerning cybercrime have becoming increasingly open to dispute. Substantial criminal provisions have obviously become a useful tool with which to protect the interests (i.e. profits) of supranational enterprises (i.e. software manufacturers, internet content providers etc.). The Council of Europe's allegedly impartial and independent legal solutions should thus be subject to immense scrutiny. Especially critical of the convention is the international coalition of NGOs co-operating in the Global Internet Liberty Campaign (GILC). The GILC has persuasively shown that the Council of Europe's legal activities are opening doors to more and more invasive criminal regulation. Dubious activities online are becoming more criminalized than their offline counterparts. The Council's legal solutions are threatening fundamental human rights and liberties, democracy and the rule of law.[17] Criticism of the Council of Europe's legal solutions is given additional fuel by its program The Project on Cybercrime, since this project is financed to a large extent by the Microsoft Corporation. The corporation has thus acquired effective control over the council's agenda and the definitional power of "problems" worth the council's attention.

DEFINITIONAL HETEROGENEITY [2.2]

Back in the 1980s computers appeared to be the pinnacle of development in the field of electronics. The term computer crime (Ger. Computerkriminalität) was thus first used in legal texts. The term was appropriate as such crime is related to computers and, since without at least two of them it is not possible to establish their connection and consequently generate the new field of human (and criminal) activity – virtual reality or cyberspace. Notwithstanding this, the term 'computer crime' is substantially and formally unsuitable. Specifying the category of crime after the means employed has not been a general practice in legal theory. Criminal legal theorists thus suggested the use of the term computer-related crime, where the fact that a computer is "only a tool in one's hands" is taken into consideration.[18] The

[16] *The Octopus Programme against Corruption and Organised Crime in Europe* began in 1996 as a joint programme of the Council of Europe and the European Commission. Since 2001, the Octopus Programme is continued by the Council of Europe as an umbrella technical cooperation programme against economic crime.

[17] GILC 2000. Similarly critical is *European Digital Rights* (EDR). See also Marzouki 2007.

[18] Brvar 1982: 94.

term was understood to encompass two elements: either a computer had to be used as the means or object of an attack, or the committing of a crime had to result from the perpetrator's expert knowledge of computer or information science. Considering the fact that expert knowledge was considered as an essential element, some criminal experts recommend the use of the term crime in information science (Fr. la criminalité informatique).

The term computer crime and its derivatives are today considered either too narrow or to denote only the first generation of cybercrime.[19] Computers and their components – microprocessors –are omnipresent: one can find them in hand watches, domestic appliances, vehicles etc. Technologies developed later are based on the transmission of data between computers and enable communication. Instead of the term 'computer' a more generic term, information-communication technology (ICT) appears to be more adequate. Besides computers the ICT development brought forth other terminal devices such as mobile phones, palms, automated network interfaces and other hybrid technologies that are bringing together existing separate technologies (TV, radio, video, telephony, satellite navigation etc.). The common denominator of these technologies has become the presence of data and a network – hence the term ICT crime.

Amongst many ICT networks the internet is a specific network that uses a special communication protocol - internet protocol (IP). Furthermore there are many ways of communicating within the internet itself: through the world wide web service (WWW) enabling access to web pages, email accounts, internet chat services (for instance programs like internet relay chat – IRC and Googletalk), the transfer of files (File Transfer Protocol – FTP), internet telephony (Voice over Internet Protocol – VoIP) etc. Hence the term internet crime (Ger. Kriminalität im Internet), e-crime or even virtual crime and computer network crime. All these terms are used in sociological discourse and are less adequate for application in the legal field, especially in criminal law with its legality principle and its component lex certa being the regulating principle. One can find also a notion of information crime, a concept wider than cybercrime as it covers not only computer crime but also fields in which computers are not present.

[19] For instance Wall 2007, *passim*.

The vast influence of the Council of Europe's Convention on Cybercrime has petrified the term cybercrime (Fr. le cybercrime, la cybercriminalité, Ger. /also/ Cyber-Crime) in legal discourse. The term is nevertheless not entirely appropriate or perhaps even logically indispensable. As already mentioned, the notion of cybernetics is originally an artistic and literary concept. The etymon of the term is the Greek kybernetes (Κυβερνήτης) for 'steersman', 'governor', 'pilot', or 'rudder', with the same root as government.[20] One can find cybernetics in medicine (for instance biocybernetics), biology, mathematics, physics, psychology, sociology, semiotics and other areas. Therefore in the criminal legal discourse the term can be problematic as lex certa is the regulating principle of criminal law.

Finally, the term high-tech crime has also entered legal discourse. The term allows a variety of new forms of technology to be regulated by, but it is very ambiguous nevertheless. Technical sophistication (the "height" of "high-tech") is surely a quality also of biotechnology, nanotechnology, nuclear, chemical etc., technologies that have very little to do with cybercrime.

CONCLUSION [2.3]

A unified and widespread definition of cybercrime still does not exist. Although the incriminations from the Convention on Cybercrime are powerful tools for harmonising the fight against cybercrime, legislators (bearing EU legislation in mind especially) use a variety of terms.[21]

Despite the differences in definitions, the fundamental characteristics of cybercrime are: technical complexity (filling one with a sense of safety on one hand and fear of "big brother" on the other), rapid development (enlarging vulnerability and extending the possibilities for infringements) and

[20] *The Cambridge Advanced Learner's Dictionary* defines cybernetics as »the scientific study of how information is communicated in machines and electronic devices in comparison with how information is communicated in the brain and nervous system«. *The Compact Oxford English Dictionary* defines cybernetics as »the science of communications and automatic control systems in both machines and living things«.

[21] For instance the Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime [COM(2000) 890 final] defines computer-related crime "as any crime involving the use of information technology". "The terms 'computer crime', 'computer-related crime', 'high-tech crime' and 'cybercrime' share the same meaning in that they describe a) the use of information and communication networks that are free from geographical constraints and b) the circulation of intangible and volatile data."

cryptography (as a protection measure and an obstacle for the detection of perpetrators). Novelties in the notion of cybercrime include the following features:
(1) a new (the virtual) crime scene;
(2) a dispersal of deviant behaviour: this involves old forms of deviant behaviour in new forms (i.e. data theft) and completely new forms of crime (i.e. cracking, hacking, computer attacks with worms and viruses);
(3) new methods for investigating crime (law enforcement) and new rules for jurisdiction and punishment (e-jurisdiction and e-punishment).

Finally the definition of cybercrime that is more or less accepted in legal discourse defines cybercrime (cumulatively):
(1) a crime threatening ICT – information and network safety (computer integrity crime or cybercrime in narrow sense),[22]
(2) a crime using ICT to commit conventional crime (computer-related crime) and
(3) a crime related to content, such as child pornography, hate-speech and the infringement of intellectual property rights (computer content crime).

THE PARTICULARITIES OF CYBERCRIME VICTIMIZATION [3]

Computer and telecommunication networks enable perpetrators to execute attacks that can be remote from the victims. The history of the first online attacks takes us back to the U.S. in the 1970s, at the time when the internet was not yet conceived. To put it precisely, the notion of a cyber attack as it is perceived today was an inseparable part of the process of creating the internet. First, let us focus on the characteristics of a cyber attack from the victim's perspective. Later, we will indicate some reasons for the paradoxical state of affairs which has made cyber attack such an essential part of cyberspace development.

Taken from the victim's perspective, the internationalization of IT has led to widespread victimization. In information societies, the users of high-tech equipment are corporations (i.e. companies and state bodies) and individuals. The individuals do not have the level of technical knowledge and

[22] Similarly, see the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

time needed for the maintenance of their computers (the updating of software and installation of various security programs), unlike the former group who usually have special technical staff (system administrators) whose sole concern is the maintenance of the company or institution's computer and network systems. From the data provided from Europol[23] it is clear that the most frequent victims of cyber attacks are companies, the next being state institutions. The least probable victim of such crime is the individual citizen. Therefore, the most susceptible part of our society to cybercrime is the business sector where it is estimated that approximately seventy percent of its most valuable data is primarily saved in electronic form. Nevertheless, the reasons for the corporate world and the modern political state itself being chief victims of cybercrime have a structural cause. The hacker culture which is still at the epicentre of the internet was the fuel for the internalization of the internet in the first place. Simultaneously, the hacker culture remains diametrically opposed to the "culture" of victims who pursue the goals of maximizing profit and monopolizing the benefits of their intellectual engagement in cyberspace. It is the clash of these two cultures that is generating the conflict.

A further characteristic of cybercrime is that very little of the victimisation that occurs is actually detected. The invasion of a computer is often difficult to detect at the time of the attack and usually requires software protection measures as well as appropriate technical knowledge. A "logical bomb" or a virus may only be triggered some time after it has been installed, often at or from another physical location. Especially difficult types of cybercrime to detect are spyware and data travellers, programs which travel through computers and report on their content to the perpetrator. Another elusive criminal program is the kind known as a war (fraudulent) dialer, which searches for holes in security programs and taps into the victim's computer.[24]

An interesting and complex psychological characteristic of cybercrime victimization is that which denies a service, or even denies victims their

[23] Europol 2003: 61.

[24] Computer tapping is a form of bugging that is not essentially different from eavesdropping; the main difference being that computer tapping bugs computer hardware that makes sounds while operating which are then transformed and deciphered by special devices.

status as victims.[25] As already mentioned, the vast majority of cybercrime victims are businesses and similar organisations, most frequently those from the banking and insurance sectors, and state institutions. There are estimates that up to 80 percent of cybercrime is committed by the employees of the victims ('cyber-sabotage').[26] However, the majority of victimized subjects are not in favour of disclosing the attack they suffer, since that would frequently only reveal their vulnerability and fallibility. Such revelations could damage the continued economic success of these victims, since they increase distrust in the safety of financial transactions and thus diminish public confidence. (The fallout from such disclosures is especially grave from the point of view of the political State, the objectivity and capabilities of which are the sine qua non of its activity.)[27] In other words, the secondary victimization of these subjects is greater than the primary victimization (the act committed by the perpetrator) and the grey figure of crime is estimated to be huge. These facts are naturally supportive of further criminal activities. However, these facts may serve as obstacles for criminal investigations and academic research, as so much simply remains unknown or undisclosed: for instance the subcultural particularities, such as the motives of the perpetrators, specific modus operandi etc., will be particularly difficult to uncover and analyse.[28]

Sociological positivism perceives the perpetrator as a victim of his or her environment. This thesis has surprising outlets in the cyberspace. Statistical data[29] shows that cyber attacks have been predominantly (in two out of three cases) motivated by the curiosity of the perpetrators. Researchers emphasize that this trend is changing with continued attacks becoming more severe, more damaging, better planned and more sophisticated. In spite of that human element, it is also the nature of the cyberspace itself to be extremely criminogenic due to the vagueness of boundaries separating legal

[25] By some estimates only 10 percent of cybercrime is reported. Source: URL: www.intergov.org.

[26] McGibbon 2001.

[27] In Slovenia a case of presumed cyber attack was executed in the computer system of the biggest Slovene bank, Nova Ljubljanska banka d.d. (NLB) in 2003. The bank had continually denied that a cyber attack on its online banking system (web service *Klik NLB*) had taken place, and claimed the bank's system is completely safe. The basic problem that was raised in that Slovenian case lay with the users' limited knowledge of the online business: they are generally qualified to use the online service but they have little or no understanding of the system's technical background. They are (again in the Slovenian case) left to the persuasive rhetorical power of the victim's PR representative.

from illegal and "normal" from "abnormal" conduct. Besides the "perpetrators from curiosity" there remains another group of perpetrators. The criminological thesis that the victims are very similar (in behaviour, attitudes to state authority, life style etc.) to (their) perpetrators is confirmed also in the cybercrime context. In one narrow field of cyber-deviancy, i.e. spamming, the victims in fact become perpetrators; since it is the primary victims who are flooding the internet with spam. Research has shown that 70 percent of spam comes from infected computers that in fact belong to its initial recipients.[30]

Finally, the virtual nature of cybercrime can be a victimizer in its own right. The virtual reality can distort the subject's ability to distinguish inner (and often fantastical) from outer reality, and lessen the subject's ability to coherently and adequately bind together the mental world with physical experience from the outer world. Virtual reality, in order words, fuses both domains of human experience – the internal and external. In order to protect ourselves from a rapidly altering, unpredictable and unstable reality, we develop psychological defences. But these defence mechanisms are not problematic as such; more important is how these defences are formed. The ability to distinguish between internal and external experience is an important indicator of psychosis. Psychiatric cases in which the nature of cyberspace has been the cause of psychological problems, or at least the strengthening force behind them, have already come to the attention of therapists.

---

[28] Theory has developed a variety of proposals for reform that should prevent denial of service attacks: a) making the reporting of such a crime to the police obligatory: although if we consider the obligatory involvement of the state repressive power, this standpoint is problematic. In addition, the victim itself should be the one to decide whether to involve the state as a third party to relationships one has with others. Moreover, the principle *volenti non fit injuria* in private law and the principle of *ultima ratio* in criminal law intervention are guiding principles that must also be observed in cyberspace. Furthermore, the interests of the victims must be taken into consideration, although that means the state is not intervening; b) again, making it obligatory to report a cybercrime, but only to the specialized professional agencies that would work as a mediators in the case; c) establishing platforms for discussions intended for actual and potential victims to exchange protective measures with state bodies and without disclosing the real names of concrete victims or perpetrators; the platform could also be used as an assembly centre for investigated cases, for counselling etc. The proposition seems to be especially appropriate because of the minimalistic intervention of the state on the one hand and users' free regulation of the cyberspace on the other hand.

[29] Deloitte Touche Tohmatsu & Victoria police, 1999: *Computer crime and security survey*. Quoting from: Europol 2003: 64, note 117.

[30] According to the data of Spamhaus Project, a non-profit organization that is tracking dispatchers of unsolicited e-mail (spamers) and announcing publicly their URL addresses. For more information Rowan.

Following the existing psychiatric classifications it is not possible to diagnose those troubles as addiction diseases, but only as pathological attachments. Nevertheless, the fusion of both domains of human experience, internal and external, can lead the subject to pathological attachment when one's voices and inner life are projected into the external world over the computer.[31] A good example of the influence the nature of cyberspace can have is the increasingly common diagnosis of an "on-off child". The diagnosis is used to denote an effect of uninhibited use of different sorts of keys and buttons that have imprinted themselves on the functions of the child's mind. The computer has an enormous impact on the adjustment of mental mechanisms, especially on the development of a subject's symbolisation ability.

PARTICULARITIES OF CYBERCRIME OFFENDERS [4]

In theory and in common language, the term 'hacker' was developed to denote a cybercrime offender.[32] The term was invented by the students of the famous Massachusetts Institute of Technology where the first modern computer system was built.[33] At first, being labelled as a hacker did not carry pejorative or criminal connotations, since hacking was not in itself considered a devastating or vandalising activity. In those early days, hacking was a desired and approved activity and merely one approach to computer programming. Later on, a fairly homogeneous group of hackers began to differentiate between computer programmers and "real" hackers. The latter are defined as manipulators of the whole technical system and not merely manipulators working within one area of the system with the aim of improving it. At first, the notion of hackers did not only include the manipulation of computers, but of any kind of technology with the intent of using it unconventionally. Hacking was perceived as a technically skilled activity which was carried out on behalf of a large technological system. Finally, the

[31] Williams gives an example of the kind of patient whose social world collapsed. By Williams, the patient's exaggerated use of the computer was one of his major symptoms and the computer played an important role in aggravating his illness. Williams.

[32] In the cyberpunk literature that anticipated cyberspace, cyber-offenders are conceived of as digital or consol cowboys (William Gibson). Cyberspace is in that way implicitly perceived as a Wild West, an unregulated place that is closely related to a highly masculinized conquering logic.

[33] Levy 1984.

distinction between legal and illegal activity was not an important one, since the mere manipulation of technology was sufficient to define it, in purely practical terms, as hacking.

Sociological analysts[34] of cyberspace generally claim that 'hacker culture' is built upon many highly positive and constructive values and beliefs on which depend, in turn, the complex co-operation, sharing and criticism of ideas, and general network interaction required for creative programming. The constitutive qualities of the original hacker cultures were the autonomy of projects and institutional autonomy. Turkle[35] defines hacking as an exclusive and impressive activity requiring sophisticated technical knowledge.

Hacker culture subsequently diverged into numerous co-existent subcultures. Among the most important groups from a criminological point of view are crackers. Crackers are perpetrators who use their technical skills to carry out malevolent actions and senseless vandalism. Within hacker culture itself, they are apprehended as not being "real" hackers. Under intellectual property law, one can also encounter a distinction between "black users" and pirates. The former are infringing intellectual property rights with the sole intention of acquiring a product for their own use. In contrast to these, pirates are motivated by the profit to be gained from selling on the product once they have obtained it. In accordance with existing criminological classifications, cybercrime can be classified as a 'white collar' crime. This definition takes into account the following facts. Substantial technical knowledge is required to commit such crimes. Secondly, statistical data shows that hackers on average have reached a graduate level of formal education. The usual stratification of hacker subcultures[36] is based on technical parameters and is not grounded on a personal or ideological basis. One politically driven organisation, for instance, is the Open Source Code movement. Its basic claim is that free access to software is covered by the human right to freedom of expression[37] and the right to privacy. On a personal

[34] For instance Castells 2001; Levy 1984; Turkle 1997.

[35] Turkle, S., *The Second Self: Computers and the Human Spirit*. Summarised from: Castells 2001.

[36] From an historical point of view, different periods were marked by different hacker subcultures. For instance, in the early eighties there were three predominant computer cultures, each grouped around a different type of hardware and computer language: *Arpanet* (the *Lisp* computer language), *Unix* (the *C* computer language) in *PC culture* (the *Basic* computer language). Castells 2001 and Naughton 1999.

[37] The claim of Richard Stallman, founder of the Free Software Foundation that later developed into the Free Software Movement.

basis, there are subcultures of hackers that perceive themselves as being akin tothe heroes of cyber punk literature or as rebels against the corporate takeovers of their internet service providers. In the contemporary world, the community of hackers is global, informal and virtual, although hackers occasionally meet in person at conferences. They are linked by a joint belief in the power of computer networks and by the shared aspiration of maintaining collective and common ownership over this power.

There are many general characteristics of cyberspace that affect the dynamics of the cybercrime perpetrators. The anonymity of cyberspace borrows a sense of perceived 'underground' activity which lends the activity an aura of mystery. Other important characteristics are the small physical and emotional risks involved and the low degree of perceivable harm and victimization. The place and time of the premeditated cyber offence are optional and can be reconceptualized; the detrimental consequences can be triggered from any location and can occur after a programmed delay in the near or distant future. All the characteristics mentioned above provide hackers with the minimal amount of risk and pressure possible. These characteristics encourage a sense of invincibility and omnipotence, and lend a certain incorporeality and even pliability to the complex physical world, along with a sense of disembodied freedom to the self.[38] The motives of hackers with criminal intent are similar, on the whole, to those of other kinds of perpetrator (greed, vengeance, curiosity), but for true hacks the intellectual challenge involved is the prime objective and overcoming it the main reward.[39]

From the 1980s onward, the social construction of hacking has bestowed on it a distinctively negative connotation. The elements of this connotation are manifold. Firstly, the notion of hacking is limited strictly to computer technology. It is then perceived merely as an illegal activity oriented purely towards making illicit profits. Additionally, the common perception of hackers is extremely pejorative. The archetypal image of the hacker is that of a

[38] For brilliantly phenomenological insights of hacking check Ullman 1997 and Springer 1996.

[39] The most typical activities of hackers are: e-mail stalking, spamming, dispatching of hate, obscene, threatening material and "e-mail bombs", virus infections, chat-room stalking, interrupting and offending, shaming, the scolding victims (*flaming*), dispatching offensive messages on BBSs (bulletin board system), launching rumours, giving offensive information in newsgroups, acquiring control over the computer system or over a the computer desktop, registering the activities on the computer (i.e. registering real time activities) etc.

male adolescent boy acting out his sexual fantasies or cowboy dreams through his computer. Furthermore, the boy is presented as maladjusted, untidy, living through and for the computer, compulsive, distanced from mainstream youth and therefore socially dislocated, lacking the ability to interact in the real world. The hacker is regarded as obsessive, solipsistic, selfish, pompous, but technically skilled. His goal is to overthrow the government and to disable intelligence. Finally, the hacker, as depicted in prevailing social conceptions, is shown as psychologically marginal or at the least, a freak who also feels superior to the rest of the community. That is the reason the hacker in effect opts out of the community and takes refuge in the extremely formal structure offered by the world of the computer, a world run on logical principles. And yet on the surface the hacker is not a subversive citizen. He leads a "normal" life on the whole and watches cult movies (i.e. Enemy of the State, The Matrix); he only lives his hacker life online.

Such a social construction of hacking and hackers is undoubtedly aggravated by an ideology that suits the purposes of certain social groups. The background of this kind of labelling exposes the ideological battle between the Open Source Code movement and multinational software producers; between the defenders of freely accessible computer software and the so-called "big players" pursuing the widest possible legal protection of their products.[40] However, the essential paradigm of the Open Source Code movement is cooperation and freedom, its foundation being a gift-culture rather than a profit-culture. For those holding the undoubtedly positive values incorporated in hacker culture and pursued by the Open Source Code movement, the distinction between hackers and crackers is becoming more and more essential. Media representations that describe hackers as citizens attempting unauthorized access to computers and other devastations of the "information superhighway", are in fact describing crackers. Thus, a hacker is "only" a programmer for whom computing serves as its own reward, who enjoys the challenge of breaking into other computers, but does no real harm.[41] Likewise, hackers are no different than any other "criminals" (or "outlaws", one might say) who are perceived ambivalently. On one hand, they are represented as holy figures and the last fighters for the individual's

[40] For further information about the domination in and over cyberspace see the final section of this paper, below.

freedom to information, while on the other they are perceived as the malicious demons of cyberspace who only disturb and prey upon the moral majority (the "law-abiding" middle class).

Taylor[42] carried out various researches on the nature of hacker culture, based on numerous interviews (primarily with hackers, but also with technical and custodial staff) and the analysis of particular exposed cases. He considers the common nature of hackers to be the quest they share for the pleasures to be gained from the identification of a desired artefact within a larger information system and the efficient management of the artefact. For hackers, the intelligence and cunning of their trade are objectives in themselves. These qualities also reveal a basis for a gender construction of hacker activity as being distinctly male dominated. The general perception of hackers, as it is derived from their representation in the media to statistical (criminological) data about them, reveals the archetypical figure of a hacker to be a young male offender. Hence this gender-based construction of hacking not only raises a classical criminological question of "why there are more male than female offenders", but also the question of the nature of cyberspace itself and the correspondent psychodynamics of perpetrators. Psychosexual theories explain the kind of female non-attendance in the hacker culture by asserting that the technology itself merely provides a cathartic experience to frustrated young boys who are seeking out the channels for their inclination to dominate. The theories perceive hacking as a substitute for sexual activity or as a sign of immature sexuality (sexuality where the computer is the hacker's partner and a virus their common child).[43] In this case, the technology is undoubtedly perceived as an object of libidinal investment, but the accentuated element is not the element that would differentiate hacking from any other human effort (i.e. cultural, scientific, sporting activity). Those theories on hacking are not entirely misleading, but are somewhat one-sided since they accentuate the generalization that hackers are usually boys with excessive testosterone, displaced li-

[41] Considering the fact that in this part of the article we want to analyse the hacker culture and psychodynamics of hackers and not the diverse forms of hacking, the term hacker/hacking is used as a wider term that includes all sorts of technical manipulations in cyberspace. The distinction between the various kinds of hackers/hacking activities is used only where it is essential to analyses the differences between those activities.

[42] Taylor 1999.

[43] Taylor 2002: 135.

bidinal energy, and male chauvinists who are inverting Freud's theory of penis envy into cyborg envy. Other gender-based constructions of hacking are more practically oriented. They claim that women do not engage in computer programming since the computer environment is imbued with immaturity, awkwardness and is by nature esoteric. Women are not interested in technical perfection and senseless destruction. They long for a technique and technical development that is not a purpose in itself.[44]

The conception of cyberspace as a boys' playground and source of eternal student life is male-oriented largely because the early hackers' environment was pervaded by masculine social attributes and objective concepts for males to 'conquer'. Taylor[45] illustrates the hacker's mentality as a "pioneer mentality" that depicts cyberspace as a Wild West, or alternatively a territory for safari or conquest. Perceiving this should lead us to appreciate that cyberspace does not represent a qualitatively new space mastered by a new paradigm. Instead, it simply shows that cyberspace is, culturally speaking, typically western; shot through with Christian-Judaic ethics, as is shown by the emphasis on penetrative thinking, innovation, audacity, power, courage, the breaking of habits and conventions etc.

In spite of this, early hacker culture contained qualitatively reformed counter-cultural values that vanished only later during the commercialisation of the internet in the 1990s. As the peak of the commercialisation of the internet is undoubtedly behind us, hacker culture can now be apprehended as a subculture incorporating a set of (post-modern) values and seeking to break through its virtual boundaries and into the physical world. Hacker culture has always possessed the potential to be a stronghold of freedom, styling itself as the leading opponent of control technologies and of the State's personal data collection. In the contemporary world hacker culture is not only a necessary counterweight, but also a supervisor and a reducer of the communicational power of gigantic economic corporations. It offers cultural resistance and a refuge for oppositional knowledge against the techno-fascist future.[46] The commercialisation of information technology has washed out professional crackers who are criminally oriented, and whose

[44] Taylor 2002: 131.

[45] Also the cyber punk literature contains the kind of conceptualisation of cyberspace where hackers are »console cowboys«.

[46] Ross 1991: 82.

value system is rooted entirely in a mainstream capitalist "culture" of accumulating profit. This group reflects unfavourably upon the whole hacker community. Confronting hackers, governments and the computer and security industries are reduced to fear and trembling. But in fact, this kind of pejorative and hostile conceptualisation of hacker culture enables the computer and security industries to dominate in and over the cyberspace. These then are the structural criminogenic factors of cybercrime. It is apparent that the symbolisation and conceptualisation of a particular activity in cyberspace is primarily dependent on the balance of power between the security industry and computer "underground".

STRUCTURAL VIOLENCE IN CYBERSPACE - PRIMACY OVER CYBERSPACE [5]

The internet is a socially constructed technological system. The culture of internet producers shaped the internet as a medium. Castells[47] conceptualises internet culture as a quadripartite structure joined by the ideology of freedom. At the initial phase of internet development, the internet was governed by the techno-meritocratic culture and the hacker culture, the first two parts of Castells' theoretic four-part model. Both technocrats and hackers shared the faith that the scientific and technological development was inherently positive. The hacker culture originated from academic culture, where the distinctive features were and continue to be open communication and peer-based control. Hence, hacker culture had already marked the beginning of the cyberspace development that was to follow in the next few years when it bridged the knowledge of the techno-meritocratic culture with that of the business sector,[48] thus enabling widespread expansion of the commercial use of information technology: this commercial and financial sector formed the third part of the internet culture recognisable today. The

[47] Castells 2001: 36.

[48] The business sector changed the internet into a so-called "new economy". The driving power of the internet economy became business's innovation-led approach and not capital itself – which is to say that the ideas that could be realised as a business venture were the driving power of the "new economy". The only goals that should in theory have made new companies successful and freed them from the bounds of traditional corporative capital, were the *expected* levels of profit and the speed at which they could be reached. Internet entrepreneurs thus had to unite the figure of the innovator, technologist and venture capitalist. This type of entrepreneur is characterized by excessive consumption, shallow socialisation and is more an artist then a businessman.

last part of the internet culture comprises what Castells describes as a "virtual community" (Rheingold) that represents the users of cyberspace. This consists of the values of the users of which these cyber communities are made up and who shape the various social processes connected to IT usage.

The essential cultural elements and values of the internet communities are to be found in the 1960s and in the counter-culture movement. Historical analyses of the internet show early online conferences as attempts to form a community after the counter-culture movement had failed in the physical world. Hacker culture is therefore imbued in values that were exiled from the physical world in a response to the emancipative movements of the sixties, in a "counter-revolution" carried out by the capitalist conservative powers. The values of the counter-culture united with the technological knowledge of techno-meritocratic culture, then found a productive base for development conducive to the form the hacker culture then took. The latter allowed for the incorporation of highly developed technological knowledge with freedom, pleasure, creativity and respect among peers. It also introduced an informal organisational structure,[49] the ideology of the gift culture, the principle of reciprocity and the principle of cooperation. But the commercialisation of various outcomes arising from computer programming was performed only on condition that all information regarding intellectual products (i.e. computer software) was to be freely accessible and that the free modification of products should also be allowed. These values were (and still are) in direct opposition to the prevailing logic in the contemporary world; namely, the logic of privatisation, profit orientation, formal legal protection and economic power. Within hacker culture, however, the commercialisation of and direct economic benefit from one's intellectual activity is only allowed to a partial extent. Hacker culture, then, is a typical post-modern paradigm that incorporates values of equality, independence, freedom of expression and communication. It is a paradigm that creates a free space for new ideas.

Within the field of cyberspace, a post-modern cultural paradigm has found a specific reflection in the Open Source Code movement. The movement's ideas are consistent with the structural physiognomy of the internet

[49] Informal organisations are governed by tribal elders (as for instance Linus Torvalds in the Linux system) or by collective authority switching its maintenance, co-maintenance etc. between different members of staff.

and its principal elements are essential for a proper understanding of hacker culture. The Open Source Code movement succeeded the original free software movement whose primary objective was to keep the collectively created benefits of computer programming out of governmental and corporate hands. The history of the free software movement goes back to the 1960s, when Unix programmers tried to protect the Unix system under copyright. These programmers from the famous Massachusetts Institute of Technology (MIT) first founded a Free Software Foundation (that later developed into the Free Software Movement) and suggested that copyright be replaced with what they called »copyleft«. Its major intent was that users should have free access to a software code and in exchange for it, these 'users' were expected to distribute the code of any eventual improvement they made to the software back onto the internet free of charge. The Foundation derived that right and the right of freedom of communication and the use of software from the human right to freedom of speech. Following the example of the Unix system, the programmers developed a new GNU/Linux[50] system, sent it out onto the internet, making it openly accessible and invited users to improve the version and send it back on the internet. In this way, Linux has been improved by hackers and other users. Unix, then already under copyright protection, impeded further improvements in the computer software industry. Later when the Unix Group dissolved, Microsoft was the only corporation left on the computer software market. The corporation gradually managed to monopolise the computer software market in spite of its inferior technology. The only alternative left was the GNU/Linux system.[51]

[50] The system is named after the 22-year-old student Linus Torvalds who created the Linux system on the basis of the Unix system that was protected with copyright. The latest news available to the author of this article at the time of writing (September 2005) was that Linus Torvalds also made an application for copyright protection of the Linux system (*sic*!).

[51] In the year 2001 approximately 30 million users were using the Linux operational system. The reason for its relatively low level of usage (in comparison to commercial Microsoft's Windows for instance) is its relatively complicated mode of application. This "user non-friendliness" is a consequence of the fact that the system was not developed with the goal of serving as wide a possible circle of users. Other open source code software for instance includes: the *TCP/IP protocol* that is a base of the first net system (*ARPA-INTERNET*), the *UNIX* operational system in the 1970s, modem's protocols in the development of PC nets, *WWW server* and *browser*, *Mosaic Browser* and partially the first commercial browser *Netscape Navigator*, the program languages *Java* and *Jini* (*Microsystems*), and the server program *Apache* etc.

Capitalist logic has created many dilemmas regarding the process of information technology commercialisation, especially in relation to the protection of the human right to privacy and the expansion of controlling technologies. It has also aggravated the classical question of the authority of the state (quis custodiet custodes) over the use of high-technology. The contemporary disproportion of power between the hacker post-modern culture and "digital capitalism" (Virilio) or "digital Darwinism" (Taylor) is generating structural violence in cyberspace. The predominance of the "digital capitalists"' value system is evident in many cases. The most notorious case to have reached the public eye is probably that of the Echelon[52] project. Echelon was a global electronic spy system intended to control communications within the internet and mobile telephone systems. It was developed by the U.S., Great Britain, Canada, Australia and New Zealand. This sophisticated spying system took the advantage of and exploited the data collecting electronic technologies of that period. The governments of the above-mentioned countries continuously denied that the system existed, but as it turned out later, this "non-existent" spying technology nevertheless ensured much substantial evidence (i.e. telephone calls, bank transfers) of the terrorist attack on the USA and its planners' movements. The second case of structural violence in cyberspace is the position computer software giant Microsoft has been allowed to take on the computer software market. The corporation has become an important player in international affairs. Microsoft software provides a platform for many other programs and its products are used by individuals (for so called personal use) as well as governments all over the world. The unrivalled market share of this software giant and the massive usage of its pre-installed products represent a huge potential danger to the autonomy and privacy of the user through the "open door" left in the software. With this risk in mind, the decision of the Indian government (in 2002) and of the München municipal authorities (in 2003) to use open source code software solutions did not come as a surprise. A further alleged case involving the abuse of power incorporated into cyberspace, is that of IBM's well-known Lotus Notes software. This program provides informational support for organisations by providing an internal communication net and a simultaneous database. A particular database contains all the doc-

[52] See also Barney 2001.

uments of a particular user (for instance all the documents of particular state agency) in digital form. For the protection of saved data, the program contains special cryptographic technology the secureness of which can be seen from the length of its cryptographic keys. However some data shows that the American National Security Agency (NSA) has partial access to the cryptographic key of the European version of this software and that this information enables the NSA to view and control users' communication and databases.

The machinations and malversations of digital capitalism in cyberspace are, then, immense and immeasurable. Yet despite the fact that exclusivist and pro-privatisation thinking is obviously also dominant in cyberspace, cyberspace still remains a place of support and strength for alternative value options. As has already been stressed, the internet and information technology go hand in hand with the hacker value system. Also, the anti-globalist movement is making the most of cyberspace's web-like structure, which perfectly suits the movement's dispersed nature. The internet represents a means of connection between the supporters of alternative value systems as well as a weapon against the reallocation of power and wealth.[53] Hacktivism as a fusion of political activism and technology is thus becoming a means of disobeying the state. It includes the problems of "real" societies, connecting abstract cyberspace with the physical world and attempts to invert the evolution of cyberspace and cyber community from the techno-liberalism into an authentic idea of hacking.

[53] The first case of the political usage of the internet and the first cyber war is considered to be the resistance of the aborigine peoples and the struggle of their representatives Zapatistas in Chiapas (Mexico) against the occupation of the Mexican government in 1994. With the use of the internet the Zapatistas' struggle became well-known all over the world; with the help of the internet they won support from various parts of the world: they now use the internet as a language learning tool, a tool for learning their customs, history etc. In that way they are lessening the impact of the Mexican government's censorship and are developing their community beyond the borders of the Chiapas. But the Mexican government also used the internet to mount a counterattack, with accusations that the Zapatistas had committed cybercrime acts (hence the reason why these struggles have become known as the first cyber war). The battle in that way furnished the first globally known example of how online communication could be used successfully for liberal political purposes, raising international support for liberation movements, internet support for anti-globalist movements (the Zapatistas' liberation movement is considered, in fact, to be the first anti-globalist gathering), widening awareness of movements for female emancipation movement and organisations campaigning for the rights of aboriginal peoples. Cere 2002.

CONCLUSION [6]

From the criminological point of view, cyber-reality is extremely paradoxical. Deviancy and the transgression of "normal" practices and values is something inherent to all stages of cyberspace development and to hacker culture. Technical excellence gained paramount importance to hackers only because their culture transcended the concepts of exclusivity, private ownership and copyright. The openness of cyberspace was always something that was culturally determined and an inherent part of the hacker culture. In addition, the management of the internet has also been collective; the development of protocols, consensus about the standards and distribution of domain names has always been accompanied by coordination and cooperation among users. A communitarian approach to technology, the meeting of meritocratic culture and utopian counter-culture, self-evaluation and peer-review, and the outlining of the internet by its use have led to unimagined developments in cyberspace. But when the cultural background of cyberspace is set down on the Procrustean bed of modern ("digital") capitalism values a number of paradoxes appear. On the one hand cyberspace holds great potential for a subject to escape culturally mediated and imposed identity patterns, but on the other hand, it is a place of isolation and passivity for the subject. Cyberspace is a place where existing communities and social ties are irrelevant, a place of "emotion inflation", but it is also a place where new communities can be formed. It is a place where patriarchal, colonialist and sexist patterns and values are perpetuated, but it is also a place that enables triumph over archaic values. It is a place where minorities are still stigmatised and marginalised, yet at the same time one that allows for the normalisation and destigmatisation of otherwise deviant conduct.

This article has dealt with the particularities of victimisation and victims in cyberspace on the one hand, and the perpetrators on the other hand. The analysis of the last inevitably triggers the necessity to highlight the cultural background of cyberspace and its wider value connotations. In spite of the progressive commercialisation of cyberspace and the distortion of its values from counter-cultural to capitalistic norms, the spirit of punk rebellion imbedded in cyberspace has not disappeared. Anti-globalist movements are using the internet as the post-modern medium par excellence to attack the

symbols of globalised, consumer, "digital" capitalism; to attack banks and the military machinery (such as the Pentagon)[54] that at first enabled the blooming of the "information superhighway" by its financial support and tolerance of the techno-meritocracy's autonomy. In these terms cyberspace has, despite of the loss of its mythical power to sublimate libidinal energy, remained an important carrier of alternative values and kept alive the potential for social change.

[54] For instance BBC 1999.

LITERATURE

[1] Ashenden, D. (2002). Cyber Terrorism and the Threat to Critical National Infrastructures. Intersec, vol. 12, no. 11/12, p. 366-368.

[2] Barney, D. (2001). Say good-bye to privacy.
URL: http://www.networkcomputing .com/1222/1222colbarney.html.

[3] BBC (1999). Nato under »cyber attack«. URL: http://www.flora.org/flora.mai-not/10498.

[4] Brvar, B. (1982). Pojavne oblike zlorabe računalnika. Revija za kriminalistiko in kriminologijo, vol. 33, no. 2. p. 92–104.

[5] Castells, M. (2001). The Internet Galaxy. Oxford: Oxford University Press.

[6] Cere, R. (2002). Digital counter-cultures and the nature of electronic social and political movements. In: Yvonne Jewkes (ed.): Dot.cons: Crime, deviance and identity on the Internet, p. 153–161.

[7] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime [COM(2000) 890 final].

[8] Council of Europe (2001). Convention on Cybercrime.
URL: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[9] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. Official Journal of the European Union L 69, 16/03/2005, s. 67-71.

[10] Europol (2003). Computer-related crime within the EU: Old crimes new tools; new crimes new tools. Luxembourg: Office for Official Publications of the European Communities.

[11] GILC (2000). Eight Reasons Why the International Cybercrime Treaty Should be Rejected, URL: http://www.gilc.org/, 1.9.2007.

[12] Grabosky, P. (2001). Computer Crime: A Criminological Overview. V: Forum on Crime and Society, vol. 1, no. 1. New York: United Nations Publications, p. 35–53.

[13] Kumar Katyal, N. (2001). Criminal Law in Cyberspace. University of Pennsylvania Law Review, 149, April, p. 1003.

[14] Levi, M. (2001). »Between the risk and the reality falls the shadow«: evidence and urban legends in computer fraud. In: D. S. Wall (ed.), Crime and the Internet. London: Routledge, p. 44-58.

[15] Levy, S. (1984). Hackers: Heroes of the Computer Revolution. New York: Penguin.

[16] Lewis, T. G. (2006). Critical Infrastructure Protection in Homeland Security. Hoboken: Wiley-Interscience.

[17] Marzouki, M. (2007). ENDitorial: The 2001 CoE Cybercrime Convention More Dangerous Than Ever. URL: http://www.edri.org./edrigram/number5.12/ cybercrime-convention-dangerous, 1.9.2007.

[18] McGibbon, A. (2001). Beware the security enemy within. Network News 13 June. URL: www.vnu.com.

[19] Naughton, J. (1999). A Brief History of the Future: The Origins of the Internet. London: Phoenix.

[20] Reimer, J. (2007). FBI: Over one million computers working for botnets. URL: http://arstechnica.com/news.ars/post/20070614-fbi-over-one-million-computers-working-for-botnets.html, 20.6.2007.

[21] Ross, A. (1991). Strange Weather: Culture, Science and Technology in the Age of Limits. London: Verso.

[22] Rowan, D., Britain is flooding the world with spam. Po URL: http://www.timesonline.co.uk, 27.4.2006.

[23] Springer, C. (1996). Electronic Eros: Bodies and Desire in the Postindustrial Age. Austin: University of Texas Press.

[24] Taylor, P. A. (1999). Hackers: Crime and the digital sublime. London & New York: Routledge.

[25] Taylor, P. A. (2002). Maestros or misogynists? Gender and the social construction of hacking. In: Yvonne Jewkes (ed), Dot.cons: Crime, deviance and identity on the Internet. Cullompton: Willan.

[26] Turkle, S. (1997). Life on the Screen: Identity in the Age of the Internet. New York: Simon & Schuster.

[27] Ullman, E. (1997). Close to the Machine: Technophilia and its Discontents. San Francisco: City Lights Books.

[28] United Nations Manual on the Prevention and Control of Computer-Related Crime, 4 U. N. Doc. ST/ESA/SER.M/43-44, U. N. Sales No. E.94.IV.5.

[29] Wall, D. S. (2002). Insecurity and the policing of cyberspace, in: A. Crawford (ed.), Crime and Insecurity. Cullompton: Willan, p. 186-210.

[30] Wall, D. S. (2004). The Internet as a Conduit for Criminal Activity. V: Pattavina, A., eds., Information Technology and the Criminal Justice System, Thousand Oaks, London, New Delhi, p. 77-98.

[31] Wall, D. S. (2007). Cybercrime: The Trasformation of Crime in the Information Age. Cambridge, Malden: Polity Press.

[32] Webster, F.; Ball, K.; eds. (2003). The Intensification of Surveillance: Crime, Terrorism, and Warfare in the Information Age. London: Pluto.

[33] Williams, P. Information Technology. URL: http://www.psychoanalysis.org.uk/ paper.htm#s, 10.11.2007.