Peer-reviewed academic journal

Innovative Issues and Approaches in Social Sciences

IIASS – VOL. 6, NO. 3, SEPTEMBER 2013

Innovative Issues and Approaches in Social Sciences

IIASS is a double blind peer review academic journal published 3 times yearly (January, May, September) covering different social sciences: political science, sociology, economy, public administration, law, management, communication science, psychology and education.

IIASS has started as a SIdip – Slovenian Association for Innovative Political Science journal and is now being published by CEOs d.o.o. (Slovenia).

Typeset
This journal was typeset in 11 pt. Arial, Italic, Bold, and Bold Italic; the headlines were typeset in 14 pt. Arial, Bold

Abstracting and Indexing services
COBISS, International Political Science Abstracts, CSA Worldwide Political Science Abstracts, CSA Sociological Abstracts, PAIS International, DOAJ.

Publication Data:
CEOs d.o.o.

Innovative issues and approaches in social sciences, 2013, vol. 6, no. 3

ISSN 1855-0541

Additional information: www.iiass.com

TO FEAR OR NOT TO FEAR ON CYBERCRIME

Igor Bernik[1], Bojan Dobovšek[2], Blaž Markelj[3]

Abstract

To understand cybercrime and its various forms, one must be familiar with criminality in general. How individuals perceive crime, and how much they fear it is further influenced by news media (Crawford, 2007). Van Duyne (2009), who monitored criminality, wrote about changes which started to be noticed twenty years ago and have shaped a new Europe, a territory without inner borders, and so with more mobility and opportunities for the Europeans. But these novelties and changes in the way we work have also caused certain new problems. It can be said that perpetrators of crimes, who are no longer hindered by state borders, now know no geographical limitations. Vander Baken and Van Daele (2009), for example, have researched mobility in connection to transnational criminality. Von Lampe (2007) has established that perpetrators no longer act individually, but frequently work in cooperation with one another. Crime and mobility are being "greased" by money, and have become a part of everyday life (Van Duyne, 2009). An individual's perception and understanding of criminality is also biased on certain cultural myths in regard to crime (Meško and Eman, 2009).

Keywords: Cybercrime, Perception, Fear, Threats, Opinion

Introduction

Not only physical mobility, but also the development of information technology has further facilitated the "erasure" of borders; it is becoming more difficult to uncover and track certain illegal activities. Perpetrators thus gained access to a new world of unlimited opportunities. This is the age of cybercrime. The problem is how to accurately define criminal activities in cyber space, since interpretations are frequently based on an individual's perception of these phenomena (Wall, 2009).

[1] Igor Bernik, Ph.D. is an Assistant Professor at the Faculty of Criminal justice and Security and Vice Dean for Academic Affairs (igor.bernik (at) fvv.uni-mb.si)

2 Bojan Dobovšek, Ph.D. is an Associate Professor at the Faculty of Criminal justice and Security and Vice Dean for Research (bojan.dobovsek (at) fvv.uni-mb.si)

3 Blaž Markelj is a Lecturer at the Faculty of Criminal justice and Security (blaz.markelj (at) fvv.uni-mb.si)

We are daily provided with news about new developments in information technology and communications. The evolution of the Internet has boosted development in other areas of information and communication technology. Mobile devices and cloud computing are among the biggest technological breakthroughs, because they facilitate simple and fast connections to the Internet (Chicone, 2009; Riedy, Beros and Wen, 2011). Slovenia is not lagging behind, quite the contrary. A study "CEE TelcoIndustry Report" carried out by Gfk Group (Internet 1) in 15 Middle and Eastern European countries, put Slovenia at the top – 27,8 % of all mobile phones are smart phones.

Information technology influences all segments of life (Dimc and Dobovšek, 2010), but the extent of this influence is subject to an individual's knowledge about the usage of information technology, his awareness of the threats and consequences of cybercrime. Cybercrime provides numerous beneficial opportunities, but also dangers for the naïve users (Bernik and Prislan, 2012). Most often users, who are not familiar with the technology and are unaware of the dangers in cyberspace, waive the protection of advanced technological solutions, which could enable them to work faster, more effectively, and, above all, safely. We believe that in time increasingly more users will be able to successfully use modern technology, and that issues of security online will no longer be overlooked. In part news media can be blamed that advanced technological solutions are not put to better use. Unprofessional reporting misleads users and forces upon them misperceptions regarding the usefulness of cyberspace and makes them fearful even though technology is relatively safe to use (Bernik and Meško, 2011).

Cybercrime should be analysed from at least two standpoints – one of the victim, the other of the perpetrator. Also to be considered are the specific circumstances in which a crime was carried out and the fear of criminality which influences public perception of and reactions to negative incidences. On the one hand, there can be no fear until people are aware of the threats, but on the other, excessive sensibility to deviant behaviour can lead to exaggerated reactions to information security threats (Završnik, 2010: 120). The fear of cybercrime is related to an evaluation of personal danger and an estimate of the cost of mitigating the damaging consequences if one becomes a victim of cyber criminals (Meško, Hirtenlehner and Vošnjak, 2009: 293). In regard to this there is a discrepancy between the statistical data on cyber crime (under-reported), the influence of news media, and the personal experiences of individuals active in cyberspace.

The Perception of Cybercrime

To better understand the situation of perception of cybercrime in Slovenia we have been carried out two studies of cybercrime in 2010 and in 2011 (Dimc and Dobovšek, 2010; Meško and Bernik (2011). The goal of the first study was to probe the public's awareness of cybercrime and the second study was to gauge public fear of cybercrime, and was carried out with the help of an Internet questionnaire addressed to the sample population. Speaking of a user's experience of cyberspace, we cannot overlook the questions, how much time people spend at the computer and why they use them (Table 1). The answers to these questions shed light on how individuals perceive cybercrime and why so.

Table 1: Daily use of a computer

Hours of use of:	> 1	1–2	2–4	4–8	< 8
A computer	11,6 %	21,3 %	33,2 %	26,7 %	7,2 %
The Internet	20,9 %	26,7 %	31,4 %	16,6 %	4,3 %

Source: Gorazd Meško, Igor Bernik

Table 2: How safe is it to use cyberspace for certain purposes?

It is safe/unsafe to use the computer for (multiple answers):	Safe	Unsafe
Internet data exchange	61	216
Downloading music/video	71	206
E-banking	78	199
Instant messaging	82	195
Online shopping	87	190
Exchange of e-mail	102	175
Random Internet browsing	114	163
Entertainment purposes (random software)	134	143
Playing online games	141	136
Business purposes (random software)	162	115
Targeted Internet browsing	172	105
Exchange of corporate data	173	104
Work	178	99
Viewing films, listening to music	184	93
Reading e-books/e-articles	203	74
Employing Office tools	229	48

Source: Gorazd Meško, Igor Bernik

As is evident, most respondent use computers and the Internet for 2 to 4 hours daily. A little more than half of this time is spent at a computer in the working place (52,3 %), 47,7 % of the time is used up for personal

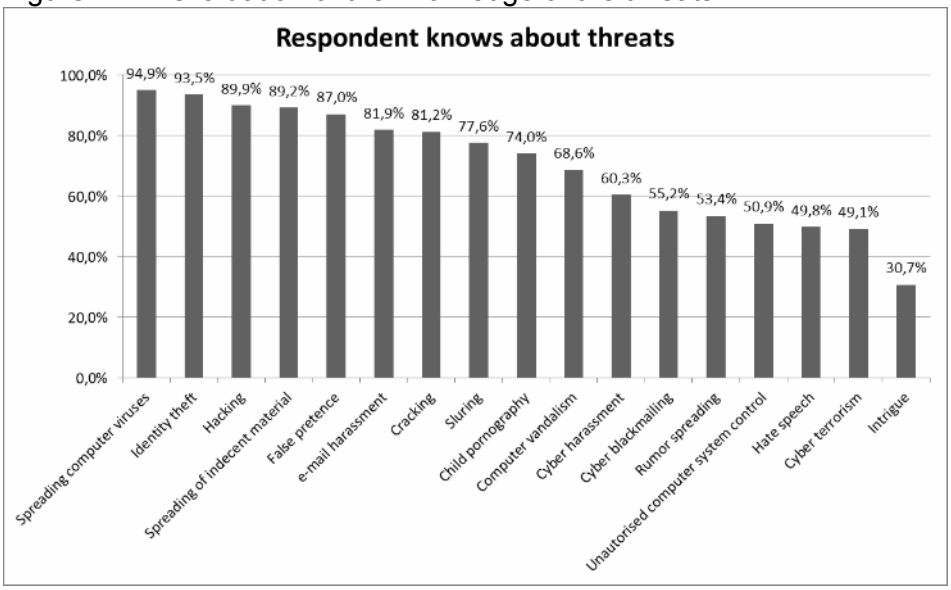
reasons. 27 % of our respondents believed that the general public has a clear understanding of where legal use of the information communication technologies ends and illegal use begins. In the attempt to touch on the issue of the borderline between legal and illegal online activities, we asked about the difference between stealing a movie in a store and illegal movie downloading. The majority of the respondents (65 %) believed that there is a major difference and the reason stated most often is the fact that downloading is socially acceptable. Also interesting is the perception that the responsibility lies with the person publishing the material, namely the person that made the material available, as stated by 19 % of the respondents.

Besides being aware of the numerous benefits of using cyberspace, one should also give thought to various threats 'lurking' in cyberspace. How aware a user is of the potential dangers depends on how well he knows their sources and how risky he thinks working in cyberspace is. It should be stressed that the most recent studies (Ponemon, 2011) showed that users are considerably exposed to cyber criminals and that the cost of eliminating damaging consequences are relatively high. Indeed, the number of incidences is steadily growing or they are perhaps being monitored more systematically. The results of the above mentioned study (Ponemon, 2011) showed that there have been 44 % more cyber attacks in 2011 then the year before.

Users believe that using computers for work, exchange of data and browsing multimedia contents is mostly safe, but relatively unsafe when they are directly connected to the Internet and are downloading general data (Table 2).

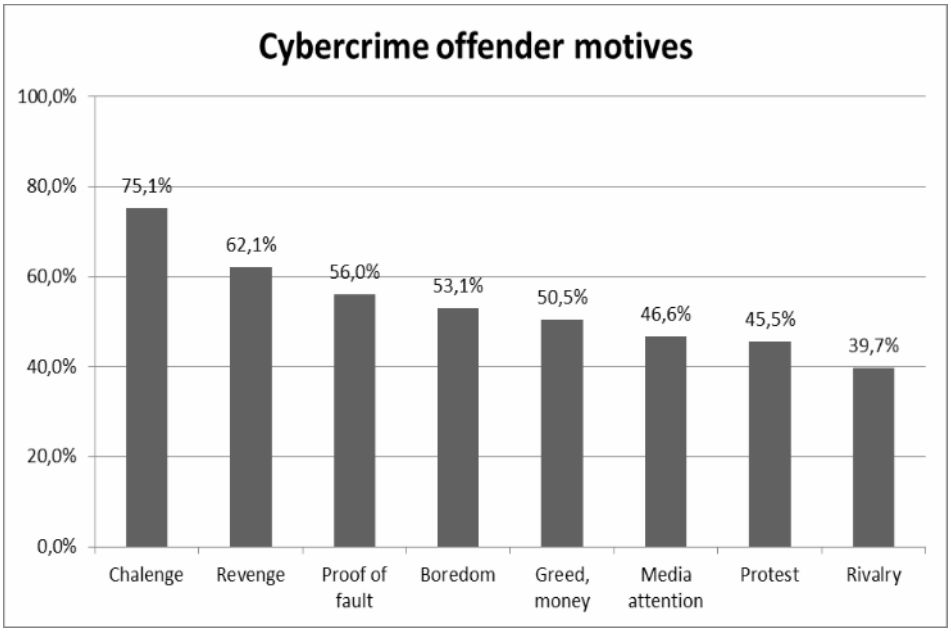
The respondents in the study answered multiple-choice questions, which were ranked numerically, about how well they are informed of cyber threats. Various categories were offered and the respondents had to mark the ones they were familiar with or had already experienced. From an overview of their evaluations of the dangers (Figure 1) it is possible to conclude that most of the respondents were aware of the threats.

Figure 1: An evaluation of the knowledge of the threats



Source: Gorazd Meško, Igor Bernik

Figure 2: Evaluation of the motives perception of perpetrators in cyberspace



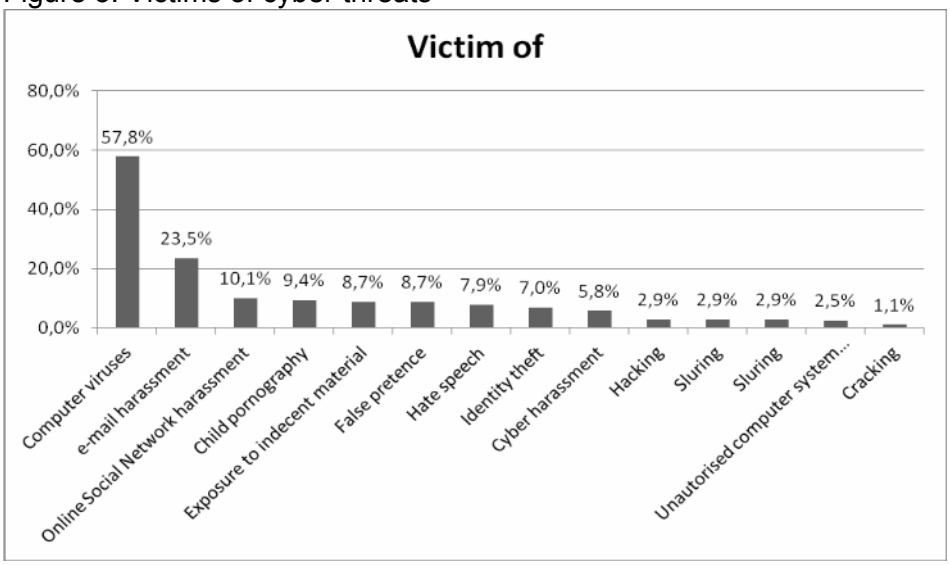
Source: Gorazd Meško, Igor Bernik

Table 3: Factoring analysis of possible threats in cyberspace

Cronbach's Alfa quotient: 0.945, Kaiser-Meyer-Olkin's quotient of sample reliability: 0.909					
F1: Inappropriate behaviour					
Cronbach's Alfa quotient: 0.914, Variance percentage: 53.833 Average value: 2.7092; standard deviation: 0.92751					
	F1	F2	F3	Arit. centre	Deviance
Spreading rumours	.830			2.7619	1.0403
False impersonation	.818			3.0586	1.0986
Hate speech	.729			2.5182	1.0092
Identity theft	.674			3.4908	1.0383
Intrigues	.614			2.3650	0.8516
Child pornography	.584			2.6423	1.0631
Cyber terrorism	.544			2.5927	1.0383
Slander	.479	– .456		2.4396	0.9785
F2: Harassment					
Cronbach's Alfa quotient: 0.901, Variance percentage: 8.827 Average value: 2.3109; standard deviation: 0.98861					
	F1	F2	F3	Arit.centre	Deviance
E-mail harassment		– .891		2.1745	0.8502
Cyber harassment (social networks)		– .887		2.2000	0.8407
Extortion in cyber space		– .802		2.2299	0.8961
Distribution of indecent material on the Internet	.370	– .460		2.4359	1.0123
F3: Active endangerment					
Cronbach's Alfa quotient: 0.875, Variance percentage: 7.517 Average value: 3.0153; standard deviation: 0.93113					
	F1	F2	F3	Arit. centre	Deviance
Cracking			,932	2,7709	0,9075
Hacking			,887	2,7766	0,9861
Unauthorised control over a computer			,639	3,1709	0,9840
Computer viruses			,607	3,6007	0,9763
Computer vandalism, theft			,589	2,7600	0,9804

Source: Gorazd Meško, Igor Bernik

Figure 3: Victims of cyber threats



Source: Gorazd Meško, Igor Bernik

While Dimc and Dobovšek (2010) asked questions about various types/methods of cybercrime, Meško and Bernik (2010) put forth questions about the perpetrators in cyberspace and their motives. The respondents thought that people accused of cybercrime had reached the following levels of education: unfinished middle school (25,6 %), middle school (38,3 %), and university degree (34,4 %). In regard to status the respondents assumed that the perpetrators were the following: pupils (14,8 %), students (33,2 %), employees (26 %), and unemployed (26 %). Respondents also thought that 86,6 % of the perpetrators were members of the middle-class. Assumptions in regard to motives are shown in Figure 2.

Meško and Bernik (2011) have measured the fear of cybercrime. They defined three categories with distinct variables, which the respondents had to rate with numbers on a five-point scale (1 = not afraid, 5 = very afraid). The authors of study carried out a factoring analysis (main components method) in which they divided the variables into three categories of (expected factors) and used a square rotation (Varimax plus a Kaiser normalisation). The results are shown in Table 3.

The second factor shows that users are also afraid of harassment in cyberspace; the threats were ranked as follows: e-mail harassment, harassment in social networks, extortion, and distribution of indecent material on the Internet. The third factor shows the extent of active forms of endangerment, the top threat being computer viruses, followed by

unauthorised control over a computer, hacking, cracking, computer vandalism, and computer theft computer. These threats have been show as valid in the studied statistical population. Besides that, it should be noted that the values for Chronbach's Alfa quotient of reliability (higher than 0.90) is relatively high, meaning that repeated studies would yield similar results.

Data pertaining to victims of certain threats in cyberspace are shown in Figure 3. In regard to the first factor users have the impression that they could fairly easily become victims (they express fear of victimisation). The respondents mostly feared to become victim of being robbed of their identity, loss by impostors, rumours, child pornography, cyber terrorism, hate speech, slander and intrigues.

Discussion and Conclusion

Among the necessary steps that would aid efforts to prevent the increase of cybercrime cases, the majority of the respondents (36 %) in the Dimc and Dobovšek (2010) study stated that increasing the level of awareness of the general public is of the utmost importance. As the analysis of research displayed, the general public seems to be acutely unaware not only of the different types of cybercrime they could inadvertently be exposed to, but also of the actions they should take or agencies they should contact in case they become victims of a cybercrime perpetrator. Furthermore, several respondents (22 %) pointed out the necessity of providing appropriate training for law enforcement officers working in the field of cybercrime, and that more of them should be employed. This statement is linked to the opinion that monetary compensation of professionals working for the government in the field of cybercrime should be increased (6 %). In order for a professional to be successful in any area of information and communication technology, it is of imperative importance that such a professional is continuously acquiring more knowledge. Professionals working in the field of cybercrime must have a combination of technical and also legal expertise, consequently the demand for such employees is also high in the business sector; the compensation in the public sector, unfortunately, oftentimes cannot compete.

Regrettably, cyber threats are developing in step with technology. We expose ourselves to these threats every time we use information technology indiscriminately. Numerous international studies, including the ones presented here, show that the situations merits concern. Growing numbers of people are spending more of their time in cyber space and do so, by using various devices, such as personal computers, tab computers, smart phones and other mobile devices.

We should not look for solutions to the dilemma how to achieve better user protection in the direction of even more advanced information technology, but in developing ways to better inform and educate users of this technology. It is certainly good if users know and understand how new technology can be (safely) used to their advantage. People usually just wish to use devices and often forget about other issues, especially security. To ensure that cyber space becomes a safer environment for users, the public must become better informed, more aware and better trained to be able to protect their personal and/or corporate data and avoid becoming victims of cyber criminals.

Resources

Alshalan, Abdullah (2011): Cyber-crime fear and victimization: an analysis of a national survey. Available at: http://www.cse.msstate.edu/~dampier/study%20materials/NationalCrimeStats.pdf (13.4.2011)

Bernik, Igor & Meško, Gorazd (2011): Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto [Internet study of understanding of cyberthreats and fear of cybercrime]. Revija za kriminalistiko in kriminologijo. Vol.: 62, No.: 3, pp.: 242-252.

Bernik, Igor & Prislan, Katja (2012): Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem [Cyber Crime, Information warfare, Cyber terrorism]. Ljubljana: Faculty of Criminal Justice and Security, University of Maribor.

Chicone, Rhonda, G. (2009): An Exploration of Security Implementations for Mobile Wireless Software Applications within Organizations. Dissertation. Minneapolis: Graduate Faculty of the School of Business and Technology Management, Northcentral University.

Council of Europe (2001). Convention on Cybercrime. Available at: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (1.9.2012)

Crafword, Adam (2007): Crime Prevention and Community Safety. In Maguire Mike, Morgan Rodney & Reiner Robert (Eds.): The Oxford Handbook of Criminology (4th Edition). Oxford: Oxford University Press.

Dimc, Maja & Dobovšek, Bojan (2010): Perception of cyber crime in Slovenia. Journal of Criminal Justice and Security. No.: 4, pp.: 378-396.

Duyne, Petrus, C. van (2009): Old and new criminally mobile Europe. In Petrus C. van Duyne, Stefano Donati, Jackie Harvey, Almir Maljevic & Klaus von Lampe (Eds.): Crime, money and criminal mobility in Europe. Nijmegen: Wolf Legal Publishers.

Internet 1: http://www.gfk.com/group/press_information/press_releases/008894/index.en.html (6.2.2012)

Internet 2: http://www.idc.com/getdoc.jsp?containerId=prUS22871611 (10.9.2011)

Internet 3: http://www.marketresearch.com/Infiniti-Research-Limited-v2680/Global-Cloud-Systems-Management-Software-6458283/view-stat (7.9.2011)

Lampe, Klaus von (2007): Criminals are not alone. Some observations on the social microcosm of illegal entrepreneurs. In Petrus C. van Duyne, Almir Maljevic, Maarten van Dijck, Klaus von Lampe & Jackie Harvey (Eds.): Crime business and crime money in Europe: the dirty linen of illicit enterprise. Nijmegen: Wolf Legal Publishers.

Meško, Gorazd (2008): Kriminologija [Criminology]. Ljubljana: Tipografija.

Meško, Gorazd & Bernik, Igor (2011): Cybercrime: awareness and fear: Slovenian perspectives. In Nasrullah Memon & Daniel Zeng (Eds.): European Intelligence and Security Informatics Conference, Athens, 12-14 September 2011, pp.: 28-33.

Meško, Gorazd & Eman, Katja (2009): Myths about crime – what is (un)real in the real world? In Gorazd Meško, Tom Cockcroft, Adam Crawford & Andre Lemaitre (Eds.): Crime, Media and Fear of Crime. Ljubljana: Tipografija

Meško, Gorazd, Hirtenlehner Helmut & Vošnjak Ljubo (2009): Izkušnje s kriminaliteto in občutek ogroženosti v Linzu in Ljubljani - preskus kognitivne teorije strahu pred viktimizacijo. [Experiences with crime and feelings of insecurity in Linz and Ljubljana - a test of cognitive theory of fear of victimization]. Revija za kriminalistiko in kriminologijo. Vol.: 60, No.: 4, pp.: 292-308.

Ponemon institute (2011): Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies, Ponemon Institute.

Riedy, M. K., Beros, S. & Wen H. J. (2011): Management Business Smart Phone Data. Journal of Internet Law, pp:.3-14.

Rupnik, Andrej (2003): Konvencija o kibernetski kriminaliteti: »Budimpeštanska konvencija« [Cybercrime Convention: »Budapest Convention«]. Available at: http://www.ltfe.org/wp-content/pdf/Kiber_kriminaliteta.pdf (25.12.2011)

Schjolberg, Stein (2010): A Cyberspace Treaty: a United Nations Convention or Protocolon Cybersecurity and Cybercrime. Available at: http://www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf (10.8.2010)

Vander, Beken, Tom & Daele, Stijn van (2009): Out of Step? Mobility of »itinerant crime groups«. In Petrus C. van Duyne, Stefano Donati, Jackie Harvey, Almir Maljevic & Klaus von Lampe (Eds.): Crime, money and criminal mobility in Europe. Nijmegen: Wolf Legal Publishers.

Završnik, Aleš (2010): Criminal justice systems` (over)reactions to IT security threats. In Bellini Marcello (Eds.): Current issues in IT security : proceedings of the interdisciplinary conference in Freiburg i. Br./Germany, 12.–14. maj 2009 (Interdisziplinäre Forschungen aus Strafrecht und Kriminologie, Bd. I 17). Berlin: Duncker & Humblot, pp.:113–135.

Završnik, Aleš (2005): Kibernetična kriminaliteta – (kiber)kriminološke in (kiber) viktimološke posebnosti "informacijske avtoceste" [Cyber crime - (cyber) criminological and (cyber) victimological specific of "information highway"]. Revija za kriminalistiko in kriminologijo. Vol.: 56, No.: 3, pp.: 248–260.

Wall, David, S. (2009): The role of the media in generating insecurities and influencing perceptions of cybercrime. In Gorazd Meško, Tom Cockcroft, Adam Crawford & Andre Lemaitre (Eds.): Crime, Media and Fear of Crime. Ljubljana: Tipografija.