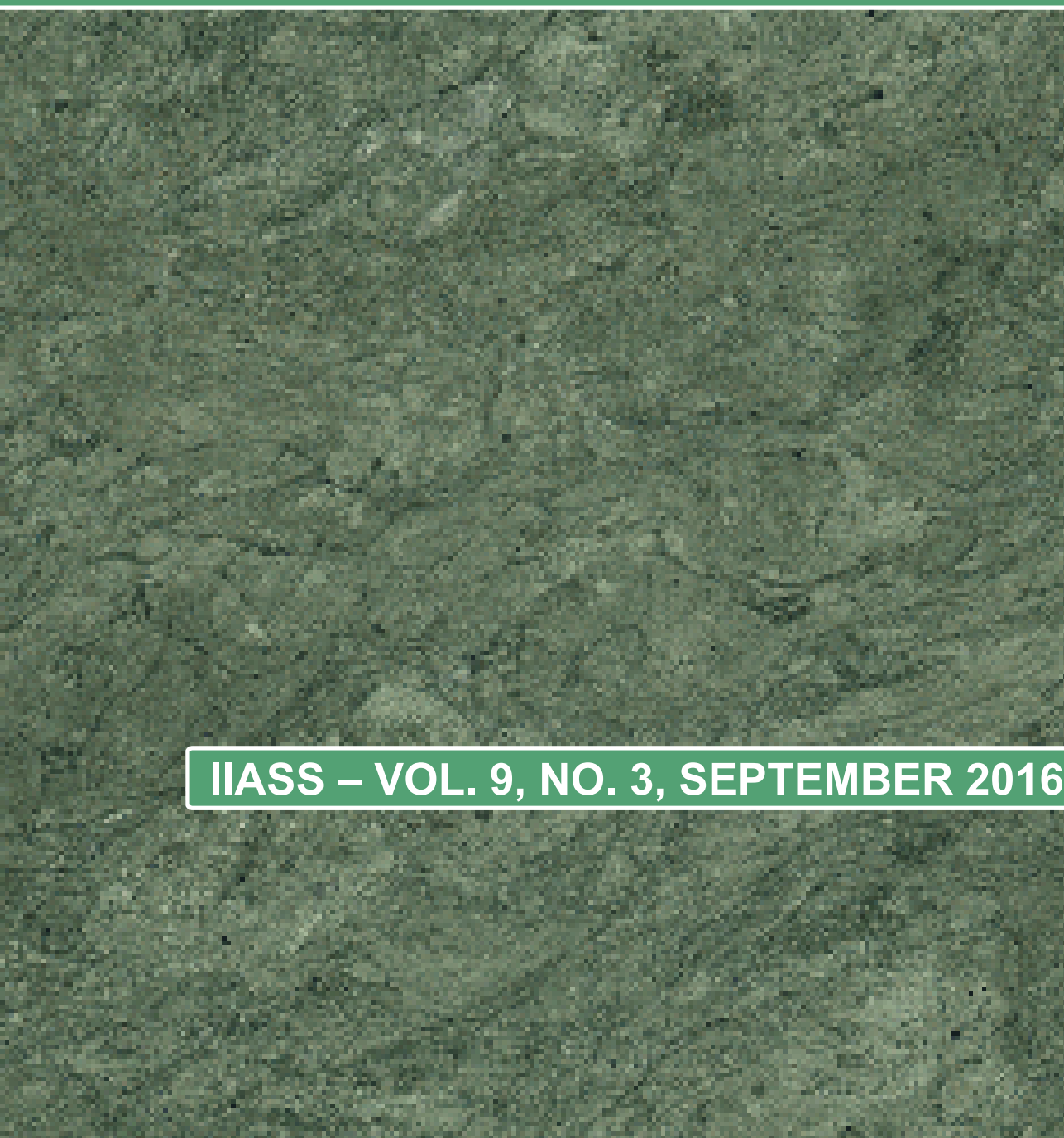
Peer-reviewed academic journal

# Innovative Issues and Approaches in Social Sciences



IIASS – VOL. 9, NO. 3, SEPTEMBER 2016

# 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 in the name of CEOs d.o.o. by Zalozba Vega (publishing house).

**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

ISSN 1855-0541

**Additional information:** www.iiass.com

# SOCIAL-ECONOMIC ASPECTS OF CYBERCRIME

Aleksandar Ilievski[1], Igor Bernik[2]



**Abstract**
The purpose of the study is to highlight the main issues of developing countries regarding cybercrime and examine the possible link between weak economic development and escalating levels of cybercrime. The findings were established on the basis of literature review, comparative studies and the synthesis of findings. The existing sociological theories of crime are not limited to traditional crime and may be used for the interpretation of its cyber version. By analysing individual sociological theories and the results of empirical research, we found that social-economic factors, such as GDP per capita, unemployment and education, are closely related to the incidence of cybercrime in different countries. This enables us to conclude that the relatively poor economic development is one of the reasons contributing to a higher incidence of cybercrime in Eastern European countries. By taking into account factors of different nature, one could increase the understanding of cybercrime and the possibility of adopting and implementing reliable preventive measures. However, this paper strives not only to understand the factors related to cybercrime, but also to raise awareness, stimulate a proactive approach and develop preventive actions in the fight against cybercrime.

**Keywords:** social-economic aspects, cybercrime, economic development.

**DOI: http://dx.doi.org/10.12959/issn.1855-0541.IIASS-2016-no3-art1**

[1] Aleksandar Ilievski, Ph.D. candidate at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research fields are cybercrime, cyber security and combating cybercrime. Contact address: *ilievski.aleksandar86@gmail.com*

[2] Igor Bernik, Ph.D., Associate Professor of Information Security and the Head of the Information Security Department at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research fields are information systems, cybersecurity, cyberwarfare, cyberterrorism and the growing requirements for cybersecurity awareness. Contact address: *igor.bernik*@fvv.uni-mb.si

## Introduction

Generally speaking, the development and enhanced functionality of information-communication technologies (ICT) have played a significant role in increasing the number of cyberspace users. Nowadays, in addition to the huge number of internet users there exist numerous electronic devices (static or mobile), that allow connection to cyberspace. Despite the presence of global connectivity to unlimited cyberspace, different countries are facing differing levels of cases of cybercrime. The purpose of the current paper is to examine one of a possible group of cybercrime factors: namely, social-economic. The authors speculate as to whether such social-economic factors can contribute to clarifying the different number of cybercrime cases around the world; in particular, the divergence between West and East world countries[3].

The United Nations Office of Drug and Crime (UNODC, 2013) ranks social-economic factors among the main factors for cybercrime. The social-economic characteristics of a country such as the level of GDP per capita, unemployment and education of its citizens paint a picture of a country's state of economic development (New Zealand government, 2011). There is a correlation between the cyber attacker's computer expertise and the degree to which a given attack is successful. Escalating levels of unemployment among people with a significant knowledge of computing and informatics might turn out to be among the important cybercrime factors. For instance, the Nigerian group "yahoo-yahoo boys" which is one of the best known cyber fraud groups in the world, is made up of uneducated young people with exceptional computing skills and expertise who live only on the profit made by frauds (Ehimen and Bola, 2010; Ojedokun and Eraye, 2012). In a very similar study Warner (2011) found that the members of the group "Sahawa boys" engage in cybercrime as a means to survive during periods of unemployment. The combination of the high number of highly educated and unemployed experts according to Kshetri (2010a) was one of the causes why Russia and the other Eastern European countries became a favourable environment for hackers. Those factors had a proven influence on flourishing cybercrime in Russia in 1998, when a large number of programmers lost their jobs and found themselves with no income (Blau, 2004).

[3] For this purpose we use the economic deffinition of East and West world countries. Therefore, the countries that are West from the borders of Austria belong in Western world countries, the others that are positioned East from the mentioned point belong in Eastern world.

The power of social-economic factors in relation to cybercrime can be explained by different social theories. Their purpose in criminology is to examine crime and deviance caused by social context. From the social perspective committing an offence not only depends upon the individual, but can also be socially conditioned (Meško, 2010). Poverty, education, inadequate housing/living conditions and the criminogenic environment are only a few of the social factors that might influence the rise in instances of cybercrime cases.

Criminological research of cybercrime can contribute not only in developing more effective actions for combating cybercrime, but also in raising the level of awareness and decreasing the risk of such threats. Regarding the influence of social-economic factors on cybercrime there exists little research. In this paper the authors define cybercrime, determine the problems of research undertaken by analysing the differences in the number of cybercrime cases between West and East world countries; they go on to employ specific social theories to explain the rise in cybercrime cases from the social-economic point of view. Based on analysis of research focussing on social-economic factors and cybercrime the authors provide guidelines for problem solving. In examining cybercrime the study takes into account only those social-economic factors that might be deemed as detrimental. Therefore, the paper highlights the main issues of developing countries regarding cybercrime, and examines the possible link between weak economic development and escalating levels of cybercrime.

**Cybercrime through cyber-attacks: variance between Eastern and Western world**

Due to the dynamic nature cyber threats, the ever-changing motivation of offenders, developments in organisation and methods of committing cyber attacks, the term cybercrime is used for a broad and complex spectrum of unlawful and immoral activities in cyberspace. A universal and widespread definition of cybercrime does not exist – precisely because of the above mentioned facts and differing views on the issue. Bernik and Prislan (2012: 9) note that “the term cybercrime is used for explaining different cyber offences including those connected with data and computer systems (hacking); with falsification and frauds, committed by using computers (phishing); unauthorized redistribution of content (sharing child pornography); and copyright infringement (distribution of pirated content)”.

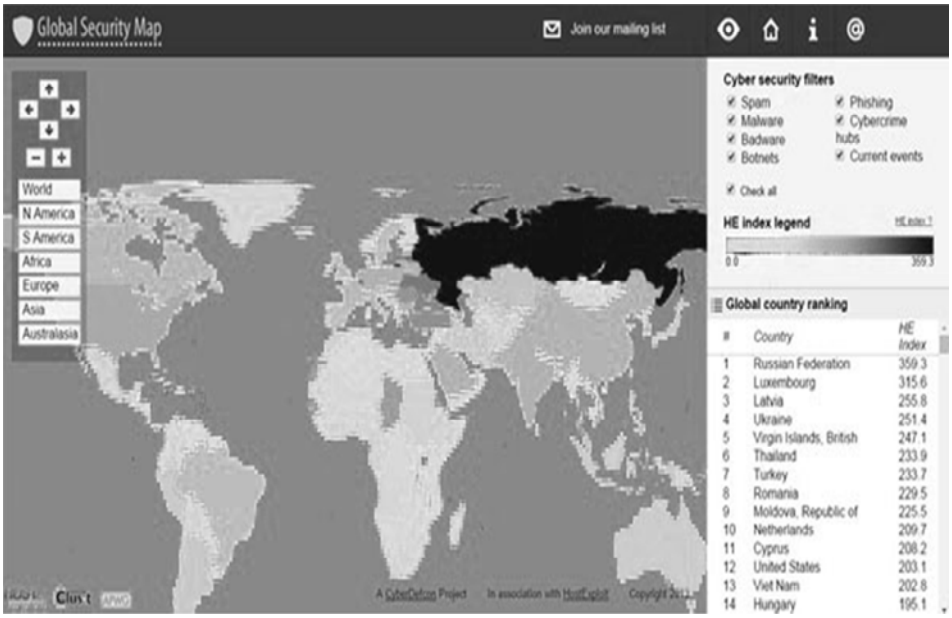
Over the past few years unlawful and harmful activities in cyberspace have been mainly committed by well-organised and innovative criminal groups. The losses of the victims of cybercrime, such as individuals,

enterprises, and countries, are continuously increasing. Norton's study (2012) found that the number of cybercrime cases in 2011 (556 million victims) exceeded the number of European Union citizens; the losses amounted to approximately 110 billion US dollars (mainly by cyber frauds). During the previous year the study (Norton, 2011) found that the number of cybercrime victims amounted to 431 million, and the overall loss was some 338 billion US dollars. Thus, five years ago the annual loss of cybercrime exceeded the value of the global black market in marihuana, cocaine, and heroin all together; that according to Norton's estimates amounted to some 288 billion US dollars. In addition, Anderson at al (2012) found, that cybercrime in addition to the directly-attributable costs, causes dramatically high indirect costs and prevention costs.

Motives for committing cybercrime offences differ; financial gain, revenge, spread of ideology, espionage, reputation increase etc. (Kshetri, 2009; Bernik and Prislan, 2012; Bernik, 2014). Despite the fact, that historically the motives of cybercrime offenders have been changing, given the damage caused and financial benefits of cybercrime cases, money is still the main motive. Modern cybercrime offenders promote the possibilities of financial enrichment, and every hacker, cracker or malware developer works for money and not only for fame and/or political reason (Kshetri, 2009). Because of the global aspect of cyberspace and the possibility of cross-border operation of such offenders, no country is immune to cyber attack. Thus, the global and unlimited space on the one hand stimulates the imagination of the offenders, and on the other it makes control over the cybercrime more complex and convoluted.

The organisation Host Exploit (Global security map, 2013) in 2009 started a project CyberDefcon, whose purpose was to present the level of cybercrime on the global basis. The main element within the project is the cybercrime index which is calculated by the organisation annually. It is based on the level of different cyber threats, such as: malware, phishing attacks, SPAM, botnets and other smaller cyber threats. On the basis of the project's results shown on Figure 1, we can notice that cybercrime is present everywhere, but with different degrees of intensity. In the group of west world countries with the highest cybercrime index fall Luxemburg, Holland and the United States of America. Russia has the biggest cybercrime index not only among the east world countries, but on the global scale. Differences between exposure to cybercrime in west and east world countries are also noticeable in the Figure 1. East world countries (particularly Eastern Europe) are taking more top positions on the global cybercrime index scale than west world ones.

Figure 1: Global exposure to the cybercrime threats




Source: Global security map, 2013.

Besides Russia, among the (Eastern) countries most threatened by cybercrime fall Latvia, Ukraine, Turkey, Moldova, and Romania (Eastern Europe countries) and Vietnam, Thailand and China (Asian countries). According to the cybercrime index report from the 2014 (Host Exploit, 2014) there are no significant deviations compared to the year before; the countries from the Eastern part of the world (particularly Eastern European) are to be found countries which top the high cybercrime index on the global scale. Significant amounts of research activities will be required to achieve a better explanation of the differences of the cybercrime level on a global basis. For that purpose, based on available social theories we wish to deeply understand the social-economic factors that might have an influence on cybercrime.

**(Cyber) crime in light of social theories**

Through social theories of crime, we are examining the possibility of explaining the different incidence levels of cybercrime threats worldwide. Strain theory is one of the most highlighted in this category. Its social context is developed through three key periods (White and Haines, 2004). During the first period, ranging from the middle of the XIX century to the early XX century, offences were viewed as being the result of social pathology and defects in the social structure or values. The second important period started in the period immediately following the

Second World War. After a few years of economic depression, the rapid development of Europe and the new Soviet Union caused mass migrations. During that period, because of an increase in the crime rate, sociologists looked for the cause of crime among the causes of migration. The findings were that unemployment and poverty were the main reasons for both migration and committing crime. Henceforward the economic circumstances of an individual began to be one of the most important crime factors. The third period of the strain theory started in the 1950s. For that period, what is typical are economic development, stable standards of living and generally an optimistic feeling about the future. Explaining the crime rate during that period presented a big challenge for sociologists. They found that factors likely to cause crime should be sought in areas such as the distribution of opportunities in society together with methods of interaction and learning.

An alternative theory which is really close Strain theory is Anomie theory. Durkheim defined the theory as the temporary position or state that occurs when society transits from a primitive to modern entity. Anomie is a consequence of widespread scientific, technical and social changes. In simplistic terms we can say that anomie is a state without norms, when norms have lost their importance and are ineffective (Meško, 2010). In some Eastern European states citizens were presented with a similar situation during the period of transition. The break with socialism during the 1990s strongly characterised the Eastern Europe countries. During this transition these countries experienced an evolution within the society. Every major social change creates a certain level of anxiety among citizens, particularly if those changes cause negative consequences such as increasing unemployment (Kossowska et al., 2012).

From the political point of view, among the Eastern European countries there emerged newcomers with no political experience – inexperienced figures who took upon themselves the political role over institutions within these countries and began to exert power, skilfully exploiting goodwill. These people were responsible for the privatisation of state enterprises, liberalization of entrepreneurial initiatives, the denationalization of previously national property, and the establishment of specific marketing standards – all of which represented a major change for the economy (Šelih, 2012). Consequently, on the one hand a small band of people in a short period of time got rich, while on the other, ordinary people were forced to look for better living conditions in Western countries. The crime rate in most of the Eastern European countries such as: Estonia, Lithuania, Latvia, Poland, Romania, Hungary etc., rose dramatically This is in contrast to Western European states

where during the same period the crime rate stayed unchanged (Kossowska et al., 2012).

Because of the aforementioned factors, Europe is still economically divided into a Western part (made up predominantly of developed countries in terms of economic status and legal system) and an Eastern part (formed mostly by developing countries with high level of unemployment, less favourable living conditions, weak legal system, etc.). In such a situation highly-educated people within society are forced to find other means and opportunities to gain financial benefits[4]. According to numerous research studies (Alganandam, Mittal, Singh and Fleizach, 2005; McCombie, Pieprzyk and Watters, 2009; Kshetri, 2010a; Kigerl, 2012), the majority of cybercrime offenders are originally from Eastern Europe and Eastern Asia. The cause of such a situation also can be explained by the Marxian Economic theory of crime. According to this theory, the source of crime derives from a country's social, and in particular, its economic system. Namely, the theory states that the genesis of crime can be trace to the individual's living conditions and to the general social conditions that cause unemployment, poverty, family misery, criminal behaviour etc. (Milutinovič, 1988).

**Cybercrime, opportunities and control**

There are further social causes which might be deemed to create so-called "delinquent subculture". According to Cloward and Ohlin, these causes derive from the discrepancy between the desires and opportunities of an individual; such an anomaly is an integral part of the Theory of Chances (Meško, 2010). People who live in less developed countries for the most part cannot achieve business success by legitimate, lawful means; at the same time, many of them kindle the "American dream" of success. Sometimes, the aforementioned strain/divergence results in the breaking the social norms and roles (Masters and Roberson, 1990).

Based on statistical data Eastern European states face a situation whereby there is a large number of unemployed and highly-educated individuals skilled in computing (Kshetri, 2010a). According to Strain theory, the likelihood of developing a delinquent subculture depends on the society and the opportunities of an individual. In countries with both poor economic and law conditions where the authorities are faced with a lack of cybercrime control mechanisms, and where citizens suffer a lack

[4] Kshetri (2010a: 1071) noted that "because of the abundance of unemployment among computing experts in Russia and other Eastern European countries, those are good environment for hackers".

of opportunities for achieving their business aspirations, there is a favourable environment for developing a delinquent subculture.

Based on defined criteria, the perpetrator of cybercrime has certain characteristics, such as (Lickiewicz, 2011: 241−243):

- Intelligence (at least average IQ and an ability to analyse and think logically);
- Personal characteristics (attention to detail and accuracy);
- Social skills (be familiar with the social norms and attitude towards other people);
- Technical skills (understanding of the operating system) and Internet addiction (spending a lot of time online).

Therefore, potential cybercrime offenders are people having highly developed technical skills, who are unemployed with weak employment opportunities. Such a thesis was proved by a Nigerian case where according to a study (Okeshola and Adeta, 2013: 104) cybercrime threats in Nigeria are very frequent mainly because of the "high level of poverty and unemployment of young people having computing education and skills". According to the same study, people commit cybercrime literally to survive.

An important factor in whether potential offenders determine to commit an offence is the likelihood/possibility of being caught by police (Meško, 2002; Jackson et al., 2012). Developing countries face a deficiency of comprehensive laws and regulations - particularly regarding cybercrime; and because of the incompetence of law enforcement agencies such states are unable to implement those laws that do exist. Developing countries have significantly fewer representatives belonging to specialized internet police services; approximately 0.2 to 100,000 internet users. That number is two to five times higher among developed countries. More than 70% of members of law enforcement agencies in developing countries report lacking computing knowledge and proper work equipment (UNODC, 2013). Such circumstances together with the high number of citizens highly educated in computing and high levels of unemployment among internet users provide favourable conditions for an increase in the number of cybercrime cases.

The influence of the lack of formal control over (cyber) crime is a major element of the Social control theory. In the same way as previously mentioned social theories, this theory also highlights the link "social role – crime". The main objective of social control is maintaining social order that may be defined as the sum of norms on which people's attitudes are based (White and Haines, 2004). Due to the complex nature of information systems as elements within cyberspace, the absence or lack

of social control over cybercrime should not come as a surprise. The connection between social control and cybercrime is also evident from studies carried out among cybercrime offenders (i.e. Ehimen and Bola, 2010; Warner, 2011; Ojedokun and Eraye, 2012). Such studies found that the sense of anonymity or absence of social control over cyberspace is one of the main factors in cybercrime.

The social-economic characteristics of countries and cybercrime are also closely linked in the Rational choice theory. This theory complements other sociological theories, particularly the Theory of chances and Social control theory. On its basis, potential offenders before deciding to commit an offence calculate/weigh up any costs that might occur (Cohen in Felson, 1979). Firstly, they count the direct costs incurred while committing an offence, such as: skills, equipment and connections. Secondly, they count the costs that might occur resulting from a jail sentence in case of arrest. Thirdly, they take into account so-called opportunity costs that result from the decision to commit an offence together with any moral factors - though from the point of view of financial moral factors are of little importance. Therefore, if the potential benefits exceed the potential losses, people decide to commit the offence. In the field of cybercrime, the aforementioned factors and influences are of minor importance. In particular, in less developed countries where the benefits of legal employment are minimal (or even do not exist), and the lack of social control decreases the possibility of sentence. Therefore, given the negligible cost of internet transactions combined with the feeling of anonymity, people using their skills may easily decide to commit a cybercrime offence.

**An empirical overview**

There are three empirical studies focussing on the social-economic factors of cybercrime. In examining cybercrime, they took into account the most highlighted social-economic characteristics, such as: unemployment, GDP per capita and education. As evident from table 1, the studies in most of the cases empirically proved the connection between cybercrime and social-economic factors.

Table 1: Influence of social-economic factors on cybercrime

| | Unemployment | GDP | Education |
|---|---|---|---|
| McCombie et al. (2009) | PH O | PH O | PH O |
| Kshetri (2010a) | OF O | OF O | OF O |
| Kigerl (2012) | SP ● PH O | SP O PH O | / |

Source: McCombie et al. 2009; Kshetri, 2010a; Kigerl, 2012
Notes: PH-phishing, SP-spam OF-online fraud

O the connection is statistically significant,
● the connection is statistically insignificant.

McCombie with co-authors (2009) found that most organised phishing attacks were committed from Eastern Europe. The main focus of the authors was to examine and establish which determinates have an influence on phishing activities in Eastern Europe. The authors focused on cybercrime in Australia; that is one of the first countries where online banking attacks were noticed. The main suspects were spammers from Ukraine. The survey is founded on case studies where individuals from Eastern Europe have been charged with related crimes. On this basis, the authors found a connection between a so-called corruption index, online penetration, level of education and cybercrime in Eastern Europe. The findings showed that the conditions in Eastern European countries are compatible with and conducive to increasing cybercrime offences. The cybercrime cases themselves indicated that individuals and groups from Eastern Europe have made significant contributions to increasing the number of phishing attacks and the other types of cybercrime worldwide. The authors noted that good technical equipment and a quite high level of education, economic instability, corruption, and poor national institutions in those countries exerted an influence on the increase of cybercrime groups and criminal cases. Kigerl (2012) focussed attention on why some countries are more vulnerable to cybercrime, particularly to SPAM and phishing attacks. The study was carried out in 132 countries in Europe, Asia, Latin America, Middle East, North America and Oceania. The author studied possible influences from different unrelated variables (number of internet users, level of unemployment, GDP per capita) on both dependent results (number of SPAM attacks and the number of phishing attacks). According to the study, unemployment does not have a direct influence on increasing SPAM attacks. Moreover, richer countries or the countries with higher GDP per capita and English speaking countries showed more SPAM attacks. In addition, according to the study, unemployment and GDP

level have a significant influence on the frequency of phishing attacks. Kshetri (2010a) is one of the rare authors who are actively researching cybercrime factors. His paper is based on the premise that the cybercrime level in developing countries in recent years has increased more than in developed countries. The study's purpose was to examine economic and institutional cybercrime factors. The author found that developing countries are faced with poor and dysfunctional means to combat cybercrime; poor legal system, weak law enforcement institutions etc. As a result of high unemployment levels and low income, the incentive/motivation to commit cybercrime increases. Using secondary data from different reports, the author found that cyber fraud mainly originated from the developing countries with high unemployment. Moreover, people living in such countries had a good knowledge/educational level in mathematics and computing; this together with the economic state of those countries, provided the conditions for an increase in the number of cybercrime crimes committed.

On the basis of our study of the social-economic aspects of cybercrime we found that the latter influence an individual's decision to commit cybercrime. Therefore, social-economic factors should be taken into consideration with regard to cybercrime etiologic and other research.

**Conclusion**

In the context of global and unlimited cyberspace, individual countries are facing differing levels of cybercrime cases. In common with the analysed results of the CyberDefcon project, which is the most trusted in the field, in our paper we found that every internet-connected country worldwide is vulnerable to cybercrime. Based on the top cybercrime index level countries for 2013 and 2014 we found that the Eastern world countries, particularly Eastern European ones (including Russia) have the highest cybercrime index level worldwide. Generally, those countries compared with their Western equivalents, are encountering poor social and economic development, high unemployment level, and poorer living circumstances.

In order to establish a theoretical basis for the higher level of cybercrime in Eastern world countries the authors have examined criminological theories that provide a social view of crime and deviant behaviour. Strain theory with its concept of three periods talks about possible social influence on crime. This theory was formulated by examining the link between "the state of society and frequency of crime" in different periods of time. The theory explains crime on the basis of three points; social pathology, weak economic state of people, and the unequal distribution

of opportunities within society. The proven high level of poverty, unemployment, and the large gap between rich and poor may increase the level of social pathology of cybercrime among the Eastern world countries. This may also be the result of the state of anomie caused during the transition periods; indeed such transitions are still present and on-going in some Eastern European countries. The absence of an economic middle class additionally upsets societal structure and the existence of highly-educated yet unemployed citizens may increase the possibility of adding to a delinquent subculture and criminogenic environment in cyberspace.

Since the (in)efficiency of law enforcement agencies also depends on the available financial resources, adverse economic conditions often influence the social control of cybercrime. The latter would be enhanced by better financial investment in law enforcement authorities thereby providing better technical equipment; maintaining cyber infrastructure properly; permanent trainee programmes for employees; better leadership and international cooperation etc. (Ilievski and Bernik, 2013). The proven absence of good social control among the less developed countries (as noted above, with two to five times fewer professional internet police officers compared with the developed countries) increases the feeling of anonymity among the perpetrators of cybercrime. According to studies of such perpetrators (Ehimen and Bola, 2010; Ojedokun and Eraye, 2012; Warner, 2011) the feeling of anonymity provides a sense of freedom in developing and committing cybercrime. If there is little or no risk of law enforcement prosecution and if people do not have any opportunity for employment, they have nothing to lose by engaging/investing in cybercrime skills/equipment for committing crime using cyberspace.

According to empirical studies we found that social-economic factors, such as GDP per capita, unemployment, and education have a statistically important influence on the increasing number of cybercrime cases. On that basis, we found that among the reasons for a greater concentration cybercrime cases in Eastern Europe might be the poor economic state and the general sluggishness in overall economic development.

The main limitation of the current paper is its focus on social-economic factors. It is already widely known that cyberspace is also used for terrorist attacks and cyber war. Such criminal activities are not only motivated by the social-economic aspect, but also political, national, religious causes etc. In order to come to a wider etiological understanding of cybercrime further studies should test also the impact

of these other possible factors. Based on the testing and analysis of different factors, society may develop more effective mechanisms and proactive actions against cybercrime. Therefore, this paper strives not only on understand the factors connected with cybercrime, but also aims to raise awareness, stimulate a proactive approach and develop preventive actions in the fight against cybercrime.

**Resources**

Alganandam, H., Mittal, P., Singh, A. and Fleizach, C. (2005). Cybercriminal activity. Retrieved from http://goo.gl/2PI7N3

Anderson, R., Barton, C., Bohme, R., Clayton, R., Van Eeten, M., Levi, M., Moore, T. and Savage, S. (2012). Measuring the Cost of Cybercrime. 11th Workshop on the Economics of Information Security. Germany: Berlin. DOI: http://dx.doi.org/10.1007/978-3-642-39498-0_12

Bernik, I. (2014). Cybercrime and Cyber Warfare. London: ISTE Ltd.

Bernik, I. and Prislan, K. (2012). Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizam. Ljubljana: Fakulteta za varnostne vede.

Blau, J. (26.05.2004). Russia - a happy haven for hackers. Computerweekly.com. Retrieved from http://www.computerweekly.com/feature/Russia-a-happy-haven-for-hackers

Chawki, M. (07.12.2005). Cybercrime in France: An Overview. Retrieved from http://www.crime-research.org/articles/cybercrime-in-france-overview/

Cohen, L. E. and Felson, M. (1979). Social change and Crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608. DOI: http://dx.doi.org/10.2307/2094589

Ehimen, R. O. and Bola, A. (2010). Cybercrime in Nigeria. Business Intelligence Journal, 3(1), 93-98.

Global security map. (2014). Cyber Defcon Project. Retrieved from http://globalsecuritymap.com/

Host exploit. (2014). World hosts report. CyberDefcon project. Retrieved from http://hostexploit.com/?p=whr-201403#download

Ilievski, A. and Bernik, I. (2013). Boj proti kibernetski kriminaliteti v Sloveniji: organiziranost, način, pravna podlaga in njeno izpolnjevanje. Journal of Criminal Justice and Security, 15(3), 317-337.

Jackson, J., Bradford, B., Hough, M., Myhill, A., Quinton, P. and Tyler, T. R. (2012). Why do people comply with the law? Legitimacy and the Influence of Legal Institutions. The British Journal of Criminology, 52(6), 1051–1071.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. Social Science Computer Review, 30(4), 470-486. DOI: http://dx.doi.org/10.1177/0894439311422689

Kossowska, A., Buczkowski, K., Klaus, W., Rzeplinska, I. and Wozniakowska-Fajst, D. (2012). In A. Šelih and A. Završnik (ed.). Crime and Transition in Central and Eastern Europe. New York: Springer.

Kshetri, N. (2009). Positive externality, increasing returns and the rise in cybercrimes. Communications of the ACM, 52(12), 141-144. DOI: http://dx.doi.org/10.1145/1610252.1610288

Kshetri, N. (2010a). Diffusion and Effects of Cyber-Crime in Developing Economies, Third World Quarterly, 31(7), 1057-1079. DOI: http://dx.doi.org/10.1080/01436597.2010.518752

Kshetri. N. (2010b). Structure of Cybercrime in Developing Economies. In N. Kshetri (ur.), The global cybercrime industry: Economic, institutional and strategic perspectives (str. 165-188). USA: Springer. DOI: http://dx.doi.org/10.1007/978-3-642-11522-6_8

Lickiewicz, J. (2011). Cybercrime psychology – proposal of an offender psychological profile. Problems of Forensic Sciences 2011, 87(1), 239–252.

Masters, R. and Roberson, C. (1990). Inside criminology. Englewood Cliffs, NJ: Prentice-Hall.

McAfee. (2009). McAfee Threats Report: Fourth Quarter 2009. Retrieved from http://www.shabakeh.net/information/articles/mcafee/EN/MC%20-%20Threats%20Q4%202009.pdf

McAfee. (2010). McAfee Threats Report: Fourth Quarter 2010. Retrieved from http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q4-2010.pdf

McAfee. (2011). McAfee Threats Report: Third Quarter 2011. Retrieved from http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2011.pdf

McAfee. (2012). McAfee Threats Report: Third Quarter 2012. Retrieved from http://www.mcafee.com/au/resources/reports/rp-quarterly-threat-q3-2012.pdf

McCombie, S., Pieprzyk, J. and Watters, P. (2009). Cybercrime Attribution: An Eastern European Case Study. Proceedings of the 7th Australian Digital Forensics Conference. Pridobljeno na http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1065&context=adf

Meško, G. (2002). Osnove preprečevanja kriminalitete. Ljubljana: Visoka policijsko-varnostna šola.

Meško, (2010). Kriminologija. Ljubljana: Fakulteta za varnostne vede, UM.

Milutinovič, M. (1988). Kriminologija: šesto izdanje. Beograd: Savremena administracija.

New Zeland government. (2011). Economic development indicators. Retrieved from http://goo.gl/FXOUMu

Norton. (2011). Norton cybercrime report. Retrieved from http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/

Norton. (2012). Norton cybercrime report. Retrieved from http://goo.gl/CMU3RI

Ojedokun. A. U. and Eraye. C. M. (2012). Socioeconomic Lifestyles of the Yahoo-Boys: A Study of Perceptions of University Students in Nigeria. International Journal of Cyber Criminology, 6(2), 1001-1013.

Okeshola, F. B. and Adeta, A. K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research, 3(9), 98-114.

Šelih, A. (2012). Crime and Crime Control in Transition Countries. In A. Šelih and A. Završnik (ed.). Crime and Transition in Central and Eastern Europe. New York: Springer.

Trend micro. (2012). Peter the Great Versus Sun Tzu. Retrieved from http://goo.gl/EYFpdt

United nations office on drugs and crime [Unodc]. (2013). Comprehensive study on cybercrime. Retrieved from http://goo.gl/Z3NuUk

United nations office on drugs and crime [Unodc]. (2011). Monitoring the impact of economic crisis on crime. Retrieved from http://goo.gl/X7xZNO

Warner, J. (2011). Understanding Cybercrime in Ghana: A View from Below. International Journal of Cyber Criminology, 5(1), 736-749.

White, R. and Haines, F. (2010). Crime and Criminology: Third Edition. New York: Oxford.