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


Publication Data:

CEOs d.o.o.

Innovative issues and approaches in social sciences

ISSN 1855-0541

Additional information: www.iiass.com
AN EXPLANATION OF THE CYBERCRIME VICTIMISATION: SELF-CONTROL AND LIFESTYLE/ROUTINE ACTIVITY THEORY

Aleksandar Ilievski

Abstract
The purpose of the current paper is to examine the causes of cybercrime victimisation, to highlight limitations of the existing cybercrime victimisation etiological studies and provide guidance for further research. The general findings are reported on the basis of a review of previous empirical studies. In addition to minor deficiencies, elements of self-control and lifestyle/routine activity theory together can be applied to the study of cybercrime victimisation. On the basis of the review of existing research, six main conclusions have been drawn. The limitation of the current research is that examines only the causes of cybercrime victimisation through the application of self-control and lifestyle/routine activity theory as the most useful for this purpose. Future research should take into account all the conclusions discussed in the paper and test new or other existing victimological theories for the purpose of better explaining cybercrime victimisation. This study contributes to improved etiological exploration of cybercrime victimisation and, consequently, to the creation of effective measures to prevent it.

Keywords: cybercrime, victimisation, self-control, lifestyle, routine activities.

DOI: http://dx.doi.org/10.12959/issn.1855-0541.IIASS-2016-no1-art02

1 Aleksandar Ilievski is a Ph.D. candidate at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research fields are cybercrime, etiology of cybercrime, cyber security and combating cybercrime. Contact address: ilievski.aleksandar86@gmail.com
Introduction
Historically, criminals always use their imagination in order to gain certain benefits by acts which deviate from social norms. On the basis of various theories, knowledge, experience and research, criminologists have explained and discussed these crimes. During the development of information and communication technologies, their abuse has confronted criminologists with new and even greater challenges. The unusual environment for the incidence of cybercrime, the lack of personal contact and the possibility of international implementation using only the "cyber highway" are only a few specific features whereby this type of crime differs from conventional ones.

Given that cybercrime is “a new and distinctive format of crime” (Yar, 2005), the application of general criminological theories to predict developments and to prevention creates new challenges (United Nations Office on Drugs and Crime, 2013). Through their everyday online activities, cyberspace users are exposed to motivated offenders. In addition to the exposure and proximity of perpetrators, users, with their risky cyberspace activities, and because they do not use adequate protective and preventive measures, could increase the likelihood of becoming a victim. Based on the lifestyle theory (Hindelang, Gottfredson and Garofalo, 1978), individuals with personal lifestyles exposed to motivated offenders increase their risk of personal victimisation. On the other hand, routine activity theory (Cohen and Felson, 1979) complements the aforementioned theory by devoting attention to the central temporal and spatial order of criminal events. Moreover, both theories focus on the impact of routine activities on the likelihood of victimisation (Ngo and Paternoster, 2011), and with some modifications this could be applied to cybercrime (Grabosky, 2001; Yar, 2005, Choi, 2008; Reyns, Henson and Fisher, 2011). Gottfredson and Hirschi (1990), in addition to situational factors, emphasised self-control as a possible individual factor in crime. Individuals with low self-control have less empathy, and their ability to perceive other people's intentions is deficient (Schreck, 1999). It is a fact that individuals who have problems perceiving intentions of others ‘face to face’ are in a much worse position in the cyber realm (Bossler and Holt, 2010), which increases their risk of becoming a victim of cybercrime.

Formal social cybercrime control is much worse than (offline) crime control (Ilievski and Bernik, 2013), which pointed out the need for more studies on the causes of cybercrime victimisation, on the basis of which we can help to combat rising threats from cyberspace. This paper carefully examines cybercrime victimization through detailed analysis of
already existing etiological\textsuperscript{1} studies in the field, in an attempt to answer the question of whether criminology theories, such as self-control and lifestyle/routine activity theory, can be applied to the study of cybercrime victimization. More reliable etiological study of cybercrime victimisation by situational and individual aspects may contribute to improving the effectiveness of that fight and to creating an early warning system, which is the main current security approach and priority of the European Union.

Criminological explanation of crime victimisation

The answer to the main victimological question about why people become victims of crime has been researching. Understanding the causes of vulnerability to crime and the endangerment of individuals through both a general theory of crime and lifestyles/routine activities theory have a central place in victimology (Holtfreter, Reisig and Pratt, 2008; Reyns et al., 2011, Prat, Turanovič, Fox and Wright, 2013). The original goal of Gottfredson and Hirschi’s (1990) general theory of crime or self-control theory has been to study the causes of delinquent behaviour. According to the theory, the main individual factor causing crime and deviance is low self-control, which is defined as the inability of an individual to exercise personal restraint in the face of tempting immediate and easy gratification, both in the short- and long-term (Hirschi, 2004).

Schreck (1999) found that self-control theory can be applied to the study of victimisation. The link between self-control and individuals’ vulnerability to crime is evident in the six elements of low self-control (Gottfredson and Hirschi, 1990): \textit{low future orientation, self-centeredness, low tolerance of frustration and anger, lack of diligence, preference for physical rather than mental activity and risk-taking}. The first dimension - \textit{low future orientation} - is believed to increase risk of victimisation because individuals without future orientation do not appreciate the long-term consequences of their actions (Schreck, 1999; Piquero et al., 2005; Williams, 2010). This dimension includes the extent of impulsive behaviour, and willingness or unwillingness to defer gratification. People with low levels of future orientation are less likely to appreciate the potential long-term consequences of their behaviour, including actions that might endanger their safety and that of their possessions (Schreck, 1999). The second component - \textit{self-centeredness} - is also associated with victimisation. Self-centred individuals are more likely to reject other’s requests and care more about their own situations and circumstances, therefore losing their support

\textsuperscript{1} According to the Oxford English Dictionary (2014), ‘etiology’ is defined as “The investigation or attribution of the cause or reason for something, often expressed in terms of historical or mythical explanation”.

A person with low empathy might also be worse at evaluating the intent of others; this, too, would increase vulnerability (Schreck, 1999; Pratt et al., 2014). The third component - low tolerance of frustration and anger – might increase risk, because acts of anger and frustration are likely to elicit counter-controlling responses from others (Schreck, 1999; Piquero et al., 2005, Williams, 2010). On the other hand, people with this shortcoming could become impatient with complex security devices, thus increasing their vulnerability (Schreck, 1999). Fourth, lack of diligence, is expected to increase victimisation, because individuals with deficiency of persistence and tenacity are unlikely to take precautions against personal victimisation (Schreck, 1999; Piquero et al., 2005; Williams, 2010). Fifth, persons who prefer physical activity are less likely to use their cognitive ability to assess a risky situation and possible responses to that situation (Piquero et al., 2005; Williams, 2010) and are therefore at greater risk of becoming a victim (Schreck, 1999). Sixth, individuals who are risk-taking are unable to avoid the risk and therefore are more likely to place themselves in situations where victimisation is likely to occur. Individuals who exhibit some of these elements are at greater risk of becoming victims.

Low self-control behaviour may be an important risk factor in victimisation, but it is only one reason people become victims (Schreck, 1999). A promising development in the same direction offers a combination of both self-control theory (Gottfredson and Hirschi, 1990) and lifestyle/routine activity theory (hereinafter LRAT) (Hindelang et al., 1978, Cohen and Felson, 1979) which provides a better understanding of the personal and situational aspects of victimisation (Schreck and Fisher, 2004; Piquero et al., 2005, Schreck et al., 2006; Holtfreret et al., 2008; Van Wilsem, 2011, 2013). Cohen and Felson (1979) with the development of the routine activity theory (hereinafter RAT) filled the gap in previous models, which do not adequately address the crime. The work of Cohen and Felson was preceded by the work of Hindelang, Gottfredson, and Garofalo (1978), as well as Amos Hawley (1950). Hindelang et al. (1978) developed “lifestyle/exposure theory”, which was based on the correlation between lifestyle choices and victimisation. They asserted that the variance in victimisation risk is related to differences in lifestyle choices. Routine activity theory is somewhat similar to lifestyle/exposure theory (Messner and Tardiff, 1985; Marcum, 2008; Marcum, Ricketts and Higgins, 2010). According to Brantingham and Brantingham (1981), Cohen and Felson sought to expand and improve on the work of Hindelang et al. (1978) by incorporating ecological concepts, specifically Hawley’s (1950) components of
temporal organisation: rhythm, tempo, and timing\(^1\). According to Cohen and Felson, the inclusion of these three components improves the explanation of how and why criminal activity is performed (Marcum et al., 2010). As asserted by Choi (2008: 310) “... these two theories, routine activities theory and lifestyle-exposure theory, are not two separate theories, but that routine activities theory is simply an expansion of lifestyle-exposure theory”. Many previous victimological studies (e.g., Messner and Tardiff, 1985; Schreck et al., 2006, Marcum et al., 2010; Ngo and Paternoster, 2011) examined victimisation on the basis of both.

Lifestyle/routine activity theory is currently the most influential and important criminological theory (Tewksbury and Mustaine, 2010). The approach is based on two simple ideas: first, the offence occurs when motivated offenders are closer to unprotected targets; second, on the likelihood of an occurrence of acts affecting our "routine activities", which include our services, family, leisure and other daily activities (DeGarmo, 2011). According to the routine activity theory, crime occurs when a motivated offender, an attractive target, and a lack of capable guardianship intersect in time and space (Cullen and Agnew, 2006).

**Low self-control and cybercrime victimisation**

In 1999, Schreck proved the theoretical and empirical links between self-control and victimisation, and since then, the study of this relationship has been developing. In addition to examining the impact of self-control on the victimisation risk of various types of conventional crime (Schreck, Wright and Miller, 2002; Unnever and Cornell, 2003; Kerley, Xu and Sirisunyaluck, 2008; Higgins, Jennings, Tewksbury and Gibson, 2009) research has also extended to the realm of cybercrime (Holtfreter et al., 2008; Bossler and Holt, 2010; Ngo and Paternoster, 2011; Van Wilsem, 2011; Vazsonyi et al., 2012; Van Wilsem, 2013). As mentioned above, individuals with low self-control often have a “here and now” mentality and place little weight on long-term consequences, focusing instead on short-term immediate gratification. They are often risk-taking and can be considered thrill-seekers. This decreases the safety of oneself and one’s property, thereby increasing vulnerability to victimisation. These same principals apply to online environments, as individuals with low self-control tend to engage in risky behaviours, such as pirating media and viewing pornography. These acts provide immediate gratification, while also increasing the likelihood of malicious software infection and other forms of victimisation. Individuals may also interact with others whom

\(^1\) Rhythm is the regularity with which events occur. Tempo is the number of events that occur per unit of time. Timing is the duration and recurrence of the events (Marcum et al., 2010).
they do not know in chartrooms and virtual environments that may lead to online harassment or cyber-stalking (Bossler and Holt, 2010).

Ngo and Paternoster (2011) found inconsistent links between self-control and the likelihood of cybercrime victimisation. Out of seven studied offences, getting a computer virus, receiving unwanted exposure to pornographic materials, being solicited for sex, encountering phishing, experiencing online harassment by a stranger and by a non-stranger, and experiencing online defamation, self-control was only significantly associated with both types of harassment. Furthermore, Bossler and Holt (2010) found that self-control has an impact on password access, changing information on one’s own computer without consent, and harassment victimisation, but not on the victimisation of malware infection or credit card fraud. For the crime types that were affected by low self-control, effects appeared to be small and indirect: people with low self-control have on average more delinquent peers, which subsequently increases their risk of victimisation. However, it is important to note that both of these studies are based on relatively small-scale, purposive samples of college graduate students. On the other hand, Van Wilsem in his two studies (2011, 2013), which are based on the general population, found that low self-control significantly increases the probability of online harassment, online consumer fraud and hacking victimisation. In the analysis of the self-control impact on fraud consumers who purchase through various electronic media (television, internet, telephone) Holtfreter et al. (2008) also found a statistical link between both. In addition to the mentioned studies, there is broader multinational research exploring the direct and indirect effects of low self-control on cyber bullying. On the basis of data from 25 European countries Vazsonyi et al (2012) found that low self-control has a significant impact on cyber bullying victimisation and perpetration.

**Cybercrime victimisation through the prism of lifestyle/routine activity theory**

The originators of LRAT (Cohen and Felson, 1979) argue that crime as a non-accidental phenomenon in society is dependent on three components: a motivated offender, a suitable target and lack of capable guardianship. Combining these elements increases the likelihood of criminal or deviant activity and increases the likelihood of victimisation (Yar, 2005). The operationalisation of the theory assumptions led to intense victimology research about various offences such as harassment (Mustaine and Tewksbury, 1999; Fisher, Cullen and Turner, 2002) sexual assault (Mustaine and Tewksbury, 2002; Cass, 2007), property crime (Fisher, Sloan, Cullen and Lu, 1998; Spano and Nagy, 2005), violent crime (Dugan, Nagin and Rosenfeld 2003, Dugan and Apel 2005).
and cybercrime (Choi, 2008; Holt and Bossler, 2008; Holtfreter et al., 2008; Marcum, 2008; Ngo and Paternoster, 2011; Reyns et al., 2011). Lifestyle/routine activities which create variable opportunity structures for successful predation always occur in particular locations at particular times, and the spatio-temporal accessibility of targets for potential offenders is crucial in determining the possibility and likelihood of an offence being committed (Yar, 2005; Reyns et al., 2011; Reyns, 2013). Yar (2005) described this requirement as a barrier between LRAT and cybercrime. The author contends that problems in the transmission of LRAT to cybercrime were caused by temporal and spatial diversity in cyberspace. However, his findings suggest that, with certain modifications, the theory could also be applied to cybercrime.

**Exposure to motivated offenders and cybercrime victimisation**

A "motivated offender" as the first element of the theory is a person or organisation that is willing to commit an offence when offered the opportunity, or when there is a suitable target which is not adequately safeguarded (Cullen and Agnew, 2006, Marcum et al., 2010, Grzybowski, 2012). An important question in examining victimisation factors is how individuals or organisations affect their exposure and proximity to motivated offenders. Marcum et al. (2010: 416) in regard to exposure to motivated offenders, states that: "..., an individual that spends more time (e.g., hours) online is more likely to be a victim, because they are exposed to other users on the Internet for a more extended period of time". Individual authors (Holt and Bossler, 2008; Marcum, 2008; Bossler and Holt, 2009) have found that in terms of studying cybercrime victimisation, this dimension is more important than the targets’ suitability and lack of capable guardianship. For offences that happen in the ‘real world’, the operationalisation of exposure to motivated offenders depends on the time that individuals spend outside the home, the time spent outside the home in the evening, the tendency to attend nightclubs or similar facilities which serve alcoholic drinks, etc. (Fisher et al., 1998, Fisher, Cullen and Turner, 2002; Mustaine and Tewksbury, 2002; Cass, 2007). Previous studies have examined whether the frequency of use of individual lifestyle/routine computer activities influence the proximity of motivated offenders to various cyber offences. More frequent spending of free time online (Alshalan, 2005, Choi, 2008; Bosler and Holt, 2009; Yucedala, 2010) is detected by various authors as a factor that increases infection with malware. Moreover, several studies conclude that more frequent use of online banking, online shopping and communication (via e-mail or instant messages) increases the likelihood of cyber bullying (Holt and Bossler, 2008; Marcum, 2008; Marcum et al., 2010; Welsh and Lavoie, 2012) and online fraud (Pratt, Holtfreter and Reisig, 2010). Van Wilsem (2011) studied the factors which affect the occurrence of any digital threats (by
Innovative Issues and Approaches in Social Sciences, Vol. 9, No. 1

e-mail or online chat) and found that the use of webcams, social networking and intensive online shopping are factors which increase the risk of victimisation. In another study Van Wilsem (2013) concluded that the above lifestyle/routine activities are significantly associated with harassment and "hacker" attacks victimisation together. His results show a considerable overlap between hacking and online harassment victimisation. In examining factors in phishing attacks and victimisation, Hutchings and Hayes (2009) found out that increased use of computers, the internet or online banking are more associated with phishing attacks than with victimisation. Ngo and Paternoster (2011) also found that the impact of an individual's online routine activities on cybercrime victimisation is limited.

Increasing target suitability and cybercrime victimisation

According to Cohen and Felson (1979), the second element of the theory – a suitable target - depends on four criteria: value, inertia, visibility and accessibility. Most cybercrime targets are informational in nature, given that all entities that exist and move in cyberspace are forms of digital code. Prime targets of this kind include the various forms of ‘intellectual property’, such as music, motion pictures, images, computer software, trade and state secrets, and so on (Yar, 2005; Yucedal, 2010). Regarding the element of a suitable target, LRAT posits that an individual’s lifestyles reflect their routine activities, and these activities, in turn, create the level of target suitability that a motivated offender assigns to that particular target (Ngo and Paternoster, 2011). Past research (e.g. Schreck and Fisher, 2004; Spano and Nagy, 2005) indicated that individuals who increase their likelihood of coming into contact with motivated offenders through exposure of their personal lives, whether with some form of contact or leaving their possessions unattended, increase target suitability.

In terms of cybercrime, many risky online activities increase target suitability and the likelihood of cybercrime victimisation. Through research based on 204 college students, Choi (2008) found that risky activities, such as frequently visiting unknown websites and downloading games, music or films, increases the likelihood of computer virus infection. Other studies (Marcum, 2008; Marcum et al., 2010) found that the examination of the data which increased target suitability had a great impact on the likelihood of receiving sexual materials, harassment by e-mail, and sexual solicitation. Namely, providing personal information to online contacts affected victimisation significantly during the high school senior period. Moreover, providing personal information on a social networking website and communicating with others online increased the likelihood of victimisation in the college freshman period, especially for
female respondents. Reyns (2013) also examined relationships between individuals’ online routines and identity theft victimisation by using data from a sub-sample of 5,985 respondents from the 2008 to 2009 British Crime Survey. His study takes account of only one risky online activity, downloading, which is found to be a significant factor, increasing risk of victimisation by approx. 30 per cent. Alshalan (2005) through an analysis of data from the 2004 US National Cybercrime Victimisation Survey found that more frequent provision of a credit card number, ID or other personal information has an impact on the likelihood of unwanted software infection and online fraud. In addition, Ngo and Paternoster (2011) found that risky online behaviours and activities such as online communication with strangers and online disclosure of personal information has a limited impact on victimisation.

**Lack of capable guardianship and cybercrime victimisation**

Lack of capable guardianship is the third element of LRAT (Cohen and Felson, 1979), which on the basis of the theory increases the likelihood of victimisation. Guardianship refers to "the capability of persons and objects to prevent crime from occurring" (Tseloni, Wittebrood, Farrell and Pease, 2004: 74). Although guardians can be both formal and informal (Yar, 2005), research which explores offences on the basis of RAT, mainly concerned the informal. Research in the field of conventional crime (e.g., Cohen, et al., 1981; Wilcox et al., 1994; Fisher, et al., 1998) mentions two dimensions of guardianship, physical and social. Physical guardianship refers to devices or objects what make it difficult to access potential victims, such as barriers, locks, alarms, and lighting on the street and in the home, etc. (Choi, 2008). Social guardianship refers to family, neighbours, friends, the density of pedestrians in the area and neighbourhood-watch programmes or the presence of law enforcement agencies (Fisher, et al., 1998). Both dimensions of guardianship could significantly reduce opportunities for committing criminal acts and individuals' victimisation risk (Miethe and Meier, 1994).

In terms of cybercrime, physical or technical guardianship relates to the use of different protective software, such as anti-virus, SPAM filters, firewalls, anti-spyware software, etc. Despite the fact that Choi (2008) concludes that the users who use anti-virus and anti-spyware software and firewalls, significantly decrease the likelihood of being infected by unwanted software, most studies (Cocotte-Muller, Elias and Morrison, 2006, Holt and Bossler, 2008; Marcum, 2008; Bossler and Holt, 2009; Marcum, 2010) conclude that the mentioned technological protection of cyber users has a limited impact on the likelihood of the same victimisation. The limited impact of technical security is not only present in victimisation by unwanted software, but also in phishing victimisation.
(Hutchings and Hayes, 2009) and cyber bullying (Marcum et al., 2010; Ngo and Paternoster, 2011). From this, it is evident that most research indicates the poor impact of technological protection on reducing the likelihood of victimisation; however, the authors (Bossler and Holt, 2009; Marcum, 2010) contend that compliance with online safety technology mechanisms are important for reducing the likelihood of victimisation in cyberspace.

Social guardianship in cyberspace in general is provided by a range of private and informal social guardians: "these range from in-house network administrators and systems security staff who watch over their electronic charges, through trade organisations orientated to self-regulation, to "ordinary online citizens" who exercise a range of informal social controls over each other’s behaviour (such as the practice of “flaming” those who breach social norms on offensive behaviour in chat rooms)" (Yar, 2005: 421). Past research on cybercrime has examined social guardianship in analysing cyber bullying victimisation (Holt and Bossler, 2008; Reyns et al., 2011; Bossler, Holt and May, 2012) and malware infection (Bossler and Holt, 2009). In terms of the above research, factors which have an impact on cyber social guardianship are directed at the location of computer use and examining how many peers have committed a certain cybercrime offence. The results of these studies suggest that social guardians significantly affect cyber bullying victimisation (online harassment and stalking), as well as the likelihood of malware infection.

Cybercrime research, in addition to both forms, also refers to personal guardianship (Grabosky, 2001; Yar, 2005, Marcum, 2008; Bosler and Holt, 2009; Ngo and Paternoster, 2011; Bossler et al., 2011; Grzybowski, 2012; Van Wilsem, 2013). In 2001 Grabosky already highlighted such protection as the most important form of defence in cyberspace (Grabovsky, 2001). Knowledge and skills in the field of computer science (as a form of personal guardianship) may have a protective role, because skilled computer users are ready to face cyber threats and risks (Bossler et al., 2011, Grzybowski, 2012). Due to different study approaches and methodology, previous research has had mixed results about the impact of personal guardianship on cybercrime victimisation. Bossler et al. (2011) found that having fewer computer skills increases the chances of harassment victimisation in cyberspace. On the other hand, studies (Holt and Bossler, 2008; Ngo and Paternoster, 2011) have indicated that good computer skills do not reduce the risk of cyber-harassment victimisation. Van Wilsem (2013) found that low computer skills were not significantly related to harassment victimisation, but closely associated with the risk of hacker
intrusions. Also, one piece of research produced totally different results than expected. Yucedal (2010) in his doctoral dissertation found a significant positive relationship between computer literacy and spyware and adware victimisation variables, which indicate that respondents who have a better knowledge of terms related to cyber threats, the internet and computers are more likely to be victims of spyware and adware infection.

**Discussion**
The current research is based on the assumption that cybercrime victimisation is not an accidental phenomenon, but depends on certain individual and situational factors. The assumption is related to one of the seven known cybercrime myths theoretically discussed by Wall (2008) which reads “Cyberspace is pathologically unsafe and criminogenic”.

After reviewing the previous research about the cybercrime victimisation causes, this paper examined the application of self-control and lifestyle/routine activity theory to the study of cybercrime and stressed some conclusions based on past research limitations which should be considered in future research.

Nowadays, self-control and LRAT are the most widely used theories for etiologically examining crime victimisation. In addition to the already proved positive impact of self-control theory on explaining traditional (offline) offences, the studies have moved to the cybercrime realm. Given the past research, it is evident that self-control theory may help in understanding victimisation in cyber realm. Having regard to the results of previous studies, people with low self-control have a greater likelihood of becoming a victim of hacking, online consumer fraud, harassment and other cyber bullying acts. Reviewing two different research papers (Bossler and Holt, 2010; Ngo and Paternoster, 2011), have been noticed that the results do not completely relate to the theory. Sampling is a possible cause of this ‘non-compliance’, because both of these studies are based on relatively small-scale, purposive samples of college graduate students. However, it is evident that, despite certain deficiencies, self-control can be applied to the study of cybercrime victimisation.

Lifestyle/routine activity theory elements (exposure to motivated offenders, suitable target and lack of capable guardianship) are also present in etiological victimisation research. Combining these elements, despite the possibility of an increase in the likelihood of criminal or deviant activities, may also increase the likelihood of victimisation. Based on a research review, it is evident that the frequency of use of certain online lifestyle/routine activities increases the user’s vulnerability
to different cybercrime offences. Current research has found that usual online activities like online banking, online shopping, communication (via e-mail or instant messages) or just more frequent internet use, affects the increasing of cyber users’ vulnerability to cyber bullying acts, malware infection, phishing attacks and other digital threats (by e-mail or online chat). However, increasing use of these activities merely escalate the user’s exposure to motivated perpetrators and do not increase his suitability as a target. On the basis of the past research, target suitability depends on using online activities which other research and reports have detected as risky. Frequently visiting unknown websites, downloading games, music or films, public disclosure of credit card numbers, ID or other personal information on social networking or other websites and online communication with strangers are activities which, based on past research, have been detected as factors which increase target suitability and consequently escalate the vulnerability of users to different cybercrime attacks.

In examining the impact of capable guardianship on cybercrime victimisation, past research considers physical or technical, social and personal points of view. Given the results of the studies presented above, it is possible to notice inconsistent relationships between technical guardians and cyber victimisation. Most research found little or no relationship between the level of using online technical guardians (such as anti-virus, SPAM filters, firewalls and anti-spyware software) and malware infection, cyber bullying and phishing victimisation. Only one research paper (Choi, 2008) found that the users who use anti-virus and anti-spyware software and firewalls, significantly decrease the likelihood of being infected by unwanted software.

Despite the fact that online social guardianship, given the ways it is provided (Yar, 2005), is so difficult to examine, certain studies (Holt and Bossler, 2008; Bossler and Holt, 2009; Reyns et al., 2011; Bossler et al., 2011) have analysed it as a factor in cybercrime victimisation. As a social guardians, the authors take into account the location of computer use and the number of peers who have committed a certain cybercrime offense. However, both variables have been proved to be factors in cyber bullying (harassment and stalking) and malware victimisation. In addition to both standard (offline) guardians, researchers have developed personal guardianship. The current study have shown that only people who have computer knowledge and skills are more able to protect themselves from individual cybercrime threats. Furthermore, we also detected differences between the results, given the limitation of the research sample.
On the basis of the review of existing research, six main conclusions have been drawn. First, research which is based on bigger general population sample found more connections between the elements of both theories and cybercrime victimisation. Second, except for one (Vazsonyi et al., 2012), other studies were conducted in one country, which calls the reliability of the studies into question. Third, the research which considered both theories (e.g. Holtfreter et al., 2008; Ngo and Paternoster, 2009; Van Wilsem, 2011, 2013) found more factors of cybercrime victimisation. Fourth, several studies (e.g. Holtfreter et al., 2008; Van Wilsem, 2011; Reyns, 2013) do not fully test all the components of the lifestyle/routine activity perspective. Fifth, individual studies (e.g. Marcum, 2008; Marcum et al., 2010; Bossler et al., 2011; Ngo and Paternoster, 2009; Reyns, 2013)\(^1\) used only a few basic or risky routine online activities which may have an impact on the final results. Finally, the cause of a non-significant link between technical guardians and cybercrime victimisation could be inadequate study. Previous research examined whether respondents had used protective software during a certain period, regardless of its updating and continuity of usage.

In addition to minor deficiencies, elements of self-control and LRAT together can be applied to the study of cybercrime victimisation. Future research should take into account all the conclusions (limitations) discussed above and test new or other existing victimological theories for the purpose of better explaining cybercrime victimisation. To conduct more reliable etiological research of cybercrime victimisation, future studies should take into account multinational comparative and longitudinal aspects. Better etiological studies of cybercrime victimisation leads to strategies and methods for recognising cyber dangers as soon as possible and the installation of early warning systems as part of today’s official security model in the European Union.

\(^1\) For instance, Bossler et al. (2011) in order to analyse respondent's online activity, asked them only about the number of hours they spend online daily. Reyns (2013) considered only downloading (films, music or games) as a risky online activity.
References


