# Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context

Mikkola, Marko

SAGE Publications Inc.
2024

Mikkola, M, Oksanen, A, Kaakinen, M, Miller, B L, Savolainen, I, Sirola, A, Zych, I & Paek, H-J 2024, 'Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context', International Journal of Offender Therapy and Comparative Criminology, vol. 68, no. 5, ARTN 0306624X20981041, pp. 449-467. https://doi.org/10.1177/0306624X20981041

http://hdl.handle.net/10138/578822
10.1177/0306624X20981041

unspecified
acceptedVersion

**This is a postprint version of the article:**

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., Zych, I., & Paek, H. J. (2020) Factors behind cybercrime victimization of adolescents and young adults: Combining Routine Activity Theory with General Theory of Crime. *International Journal of Offender Therapy and Comparative Criminology,* https://doi.org/10.1177/0306624X20981041

# Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context

## Abstract

Routine Activity Theory (RAT) and the general theory of crime have been widely employed to understand cybercrime victimization. However, there is a need to integrate these theoretical frameworks to better understand victimization from a cross-national perspective. **Method**: A web-based survey was conducted among participants aged 15 to 25 years from the U.S., Finland, Spain, and South Korea. **Results**: Factors related to RAT were associated with increased victimization in all four countries although results varied between the countries. Low self-control was associated with victimization in the U.S., Finland, and Spain but not in South Korea. Using decomposition analysis, we discovered that the association between low self-control and victimization occurred both directly and indirectly through measures of RAT. **Discussion**: Our study demonstrates the need to integrate theories to better understand the dynamics of victimization. Despite the usefulness of RAT, other theories should be taken into consideration when investigating cybercrime victimization.

**Keywords**: cybercrime, victimization, Internet, social media, routine activity theory, general theory of crime

## Introduction

The rapid development of information and communication technology has contributed to the increasing use of the Internet and social media, facilitating people's everyday life. The Internet and social media platforms offer their users many beneficial services that can ease people's daily routines. These platforms offer possibilities to create and maintain professional and personal social networks as well as share and consume information with people who have similar interests. They can also function as a source of fulfilling individuals' social and psychological needs, such as belongingness, self-esteem, and avoiding loneliness (Gonzales & Hancock, 2010; Kim, Larose & Peng, 2009; Seidman, 2013). For example, these platforms can provide opportunities to reduce loneliness and the discrepancy between desired and existing social relationships (Perlman & Peplau, 1981). Further, loneliness is an important factor in predicting an individual's psychological health (Baumeister & Leary, 1995) as lonely and depressed people tend to develop addictive or compulsive Internet behavior which can lead to other negative social outcomes such as hostility or depression (Griffiths, 2000; Kim et al., 2009; Yen et al., 2008).

According to Internet Live Stats (2019), annual user growth of the Internet exceeds global population growth. Internet Live Stats (2019) estimates that nearly 57% of people in the world are using the Internet. At the same time, the number of social media users nearly tripled between 2010 and 2017 from 0.97 billion to 2.46 billion and is estimated to exceed three billion users in the year 2021 (Statista, 2019). The use of the Internet and social media is not evenly spread but varies between regions and countries. As of June 2019, it was estimated that 89% of people living in North America were using the Internet while other parts of the world had lower percentages, with Europe at 87%, Asia at 52%, and Africa at 40% (Internet World Stats, 2019). In its

essence, the Internet may be considered a massive network of connected computers, while social media can be described as a vast network of people known and unknown to each other, interacting through the Internet (Reyns, Henson & Fisher, 2011).

The Internet with its numerous different services and social networks is not only a playground for ordinary people looking for relief from daily activities. It is also a mediating tool for criminals to engage in illicit activities and seek victims (Bossler & Holt, 2010; Marcum, Higgins & Ricketts, 2010; Yar, 2005). The increasing number of Internet and social media users means there is an increase in the opportunity to find suitable targets for those committing criminal acts online. Therefore, cybercrime has become a growing threat to people living in technically advanced countries (Meško, 2018).

Widespread routine-like usage of the Internet and social media corresponds with general crime trends where the rate of traditional crimes is decreasing (Griffiths & Norris, 2020; Office for National Statistics, 2015; Tcherni, Davies, Lopes & Lizotte, 2016), while the rate of crimes utilizing information and communication technology is increasing (Kivivuori, Aaltonen, Näsi, Suonpää & Danielsson, 2018; Office for National Statistics, 2015; Tcherni et al., 2016). This change in criminal offending is likely to result in a situation where an increasing number of adolescents and young adults are victimized irrespective of their nationality or location on the globe. Adolescents' and young adults' behavior compared with older age groups is usually more risk driven, as younger individuals are more susceptible to peer pressure leading them into high-risk behaviors, such as deviant or criminal acts (Akers, 1999; Warr, 1993). This can further lead youth to both commit criminal acts and be exposed to online offenders.

People who commit crime are also likely to become victims of crime. This victim-offender overlap is well established in previous research (Gottfredson & Hirschi, 1990; Kerstens & Jansen, 2016; Kranenbarg, Holt & Gelder 2019; Ngo & Paternoster, 2011). Crimes are typically concentrated among a small number of individuals, making it more likely that the same individuals are being repeatedly victimized (Ellonen & Salmi, 2011; Finkelhor, Ormrod, Turner & Hamby, 2005; Martinez, Lee, Eck & SooHyun, 2017). Therefore, it is important to understand the factors behind cybercrime victimization and develop new possible intervention strategies so that the cycle of victimization can be prevented as early as possible.

Previous research using established theories of crime causation have focused on online victimization, its multiple aspects, and factors behind victimization (Leukfeldt, 2014; Marcum, 2008; Ngo & Paternoster, 2011; Näsi, Oksanen, Keipi & Räsänen, 2015; Reyns, 2011). For example, Marcum (2008) using Routine Activity Theory found that among college freshmen in the U.S. ($N = 483$), exposure to offenders and target suitability increased the likelihood of cyber victimization. Whereas, Ngo and Paternoster (2011) using general theory of crime and Routine Activity Theory, found that among U.S. college students ($N = 282$) neither individual nor situational characteristics consistently impacted the likelihood of cyber victimization and low self-control was only partially related to cyber victimization. Outside the U.S., Reyns (2011) employed Routine Activity Theory in a study with British citizens ($N = 5{,}985$, age 16–91 years), and found that exposure to offender and target suitability did in fact increase the probability of becoming a victim of cybercrime.

In our cross-national study, we approach cybercrime victimization from a social psychological standpoint using the combined criminological framework of Routine Activity Theory (Cohen & Felson, 1979) and general theory of crime

(Gottfredson & Hirschi, 1990). Moreover, we examine whether both low self-control and risky online routines are associated with cybercrime victimization and whether the effect of low self-control is mediated via increased risky routines. This combined framework has been utilized in explaining offline violence victimization (Ren, He, Zhao & Zhang, 2017; Stewart, Elifson & Sterk, 2004; Turanovic & Pratt, 2014) and online victimization (Ngo & Paternoster, 2011). In our study, we test the combined framework in a cross-national setting. We focus on online victimization of adolescents and young adults in well advanced information societies with high Internet penetration percentages.

***Cybercrime***

In this study, cybercrime refers to criminal offenses such as slander, threat of violence, identity theft, fraud, or sexual harassment taking place on the Internet. As cybercriminals are not restricted by national borders, defining cybercrime becomes problematic as these crimes often span several legal jurisdictions. Moreover, because cybercrime legislation differs from one country to another, we will rely on self-report survey-data of victimization rather than jurisdiction specific legal definitions. This is feasible given the cross-national focus of the study. Utilizing this self-report approach for cybercrime is common in previous research (see Bossler & Holt, 2010; Kaakinen, Keipi, Räsänen & Oksanen, 2018; Oksanen & Keipi, 2013; Reyns et al., 2011).

In general, cybercrime involves offenses directed at individuals using computers and computer networks as mediating tools. These offending acts may range from cyberstalking and cyber harassment to hate crimes, identity theft, fraud, and threats of a sexual and violent nature (Bossler & Holt, 2010; Hay & Ray, 2019; Marcum et al., 2010; Yar, 2005). Studies show the global annual financial loss credited to cybercrime is in the billions of dollars and millions of people have fallen victim to it

(Gañán, Ciere & van Eeten, 2017; Saini, Rao & Panda, 2012). Cybercrime victimization is considered just as harmful as victimization taking place in the physical world. Wigderson and Lynn (2013) found that many forms of cybercrime are negatively associated with the well-being of adolescents and that cyber victimization can, in fact, influence adolescents more than traditional forms of victimization (see Bren & Li, 2005). A possible explanation for this is because nearly every Western adolescent has their own Internet access at home, therefore the home does not safeguard them from potential dangers (Mason, 2008). Living at home with parents does not always imply getting help from parents, especially since cyber bullying and cybercrime can go easily unnoticed (Hay, Meldrum & Mann, 2010).

***Routine Activity Theory***

One of the popular theories in crime victimization research is Routine Activity Theory (RAT) developed by Lawrence Cohen and Marcus Felson (1979). RAT is a situational theory, where crime is most likely to occur when a motivated offender and suitable target meet in a situation lacking a capable guardian. The opportunity for such a situation is created by the routine lifestyles of a suitable target, who becomes visible to the offender, and other social actors. Therefore, crime is not a random occurrence, but rather, follows the routine patterns of social life (Marcum, 2008). Also, according to the theory, there are always motivated offenders seeking suitable targets (Cohen & Felson, 1979).

RAT was originally developed to explain conventional crime in the "physical world" when a motivated offender and a suitable target meet in a situation which is lacking a capable guardian. According to Felson (2016), cybercrime follows the same principals as crime in the physical world even though an offender, victim, and capable guardian do not coexist in the same physical space and time. Space and time

will only change the nature of crime but not its meaning (Felson, 2016). Thus, RAT has been applied to a wide range of cybercrime studies over the past years (Bossler & Holt, 2009; Holt & Bossler, 2008; Holt, Leukfeldt & Van De Weijers, 2020; Marcum et al., 2010; Näsi et al., 2016; Reyns, 2011; Reyns et al., 2011).

Routine Activity Theory has also received criticism regarding its suitability to explain cybervictimization (Yar, 2013: Leukfeldt & Yar, 2016). Some studies have shown limitations of using RAT to explain cybercrime victimization, especially when the strict definitions of its three core components have been followed: motivated offender, target suitability, and absence of guardianship. This is mainly because in the digital world, suitable target and a motivated offender do not necessarily converge within a shared time and space (Leukfeldt & Yar, 2016; Näsi, Räsänen, Kaakinen, Keipi & Oksanen, 2016; Reyns et al., 2011; Yar, 2005). In earlier online victimization research, guardianship has been measured in a variety of ways, but a large portion of the research has focused on an individual's social network as a source of guardianship (Holt & Bossler, 2008; Näsi et al., 2016).

### *Self-Control in General Theory of Crime*

General theory of crime was introduced by Michael Gottfredson and Travis Hirschi in 1990 and is combined with RAT in this study. A key element in general theory of crime is self-control. Low self-control, which is commonly manifested as impulsivity (White, Moffitt, Caspi, Bartusch, Needles & Stouthamer-Loeber, 1994), has been considered to explain the susceptibility to both committing crime and being victimized in physical and digital contexts alike (Gottfredson & Hirschi, 1990; Reyns et al., 2014; Schreck, 1999; Tagney, Boone & Baumeister, 2018).

According to general theory of crime, people with low self-control tend to act impulsively and look for immediate gratification without thinking about the long-

term effects of their actions. Therefore, people with low self-control are more likely to commit crime or deviant acts than people with high self-control. Low self-control also increases the risk of victimization (Bossler & Holt, 2010; Kranenbarg et al., 2019; Schreck, 1999; Schreck, Wright & Miller, 2002). For instance, self-control can influence individual's daily routine so that they engage in activities that make them more visible to offenders, resulting in higher odds for them to become a victim of crime (e.g., Reisig & Golladay, 2019).

Because self-control and the impact of self-regulation affect the quality of individuals' life, self-control has been extensively studied in social psychology. According to previous research studies (Baumeister & Heatherton, 1996; Baumeister & Leary, 1995; Hofmann, Luhmann, Fisher, Vohs & Baumeister, 2013; Tagney et al., 2018), people with good self-control are doing well in their lives, are happier, and they face fewer hardships than people with low self-control. With strong self-control, the individual is able to control one's own behavior and see the long-term consequences of one's actions. On the other hand, low self-control is not the reason for committing crimes, but rather, strong self-control acts as a deterrent between the actor and the crime.

Individuals engaging in risky behavioral and lifestyle routine-like activities are at a greater risk of victimization both offline and online (Cohen & Felson, 1979; Felson, 2016). Earlier studies suggest that individuals with low self-control are more likely to take part in risky activities such as aggressive or delinquent behavior because they find this type of activity to be fun or exciting (Gottfredson & Hirschi, 1990; Kulig, Pratt, Cullen & Unnever, 2017; Pratt, 2016). By doing so, these individuals expose themselves as suitable targets to motivated offenders, thus increasing their risk of getting victimized in a situation lacking guardianship, both in offline and online

contexts (e.g. Kulig et al., 2017; Reisig & Golladay, 2019; Reisig, Pratt & Holtfreter, 2009; Turanovic & Pratt, 2014).

***This study***

This study aims to investigate if RAT and general theory of crime together could be used to analyze online victimization among adolescents and emerging adults cross-nationally. Moreover, we analyze whether the association between low self-control and cybercrime victimization is mediated via increased involvement in risky online routines. This theoretical framework has been utilized in earlier studies (Reisig & Golladay, 2019; Ren et al., 2017; Stewart et al., 2004; Turanovic & Pratt, 2014), but this is the first study to extend these tests and examine cybercrime victimization in a cross-national context using representative samples from four countries across three continents.

The research questions are:

1. Are routine activities on the Internet and self-control associated with adolescents' and emerging adults' cybercrime victimization?
2. Does low self-control have indirect connection to cybercrime victimization through measures of routine activity theory?

## Method

***Participants***

Participants of the study were adolescents and young adults aged 15 to 25 years who entered the study from the U.S. ($N$ = 1212, 50.2% female, $M_{age}$=20.1, $SD_{age}$=3.19) in January 2018, Finland ($N$ = 1200, 50% female, $M_{age}$=21.3, $SD_{age}$=2.85) in March–April 2017, Spain ($N$ = 1212, 48.8% female, $M_{age}$=20.1, $SD_{age}$=3.16) in March 2019, and South Korea ($N$ = 1192, 50.4% female, $M_{age}$=20.6. $SD_{age}$=3.24) in

March 2019. In order to achieve data that mirrored the current population estimates of each examined country, the data were demographically balanced for age, gender, and living area in all four countries (for details, see Oksanen, Sirola, Savolainen & Kaakinen, 2019).

***Procedure***

A volunteer participant pool managed and maintained by a global data provider company Dynata (formerly known as Survey Sampling International), was used to recruit respondents to the study. Dynata serves a wide range of industries with online data collection and robust panels. A 15-minute web-based survey was used for data collection in all four countries using previously validated measures that have been widely used in earlier comparative research. The survey was originally designed in Finnish and it was translated into English. The translation went through a back-translation process to affirm the survey's internal consistency and accurate matching of the items. Next, the English version was translated into Korean by proficient Korean and English speakers and later into Spanish by proficient Spanish and English speakers. Both, the Korean and Spanish translations went through the back-translation process to ensure internal consistency and accurate matching of the items.

***Measures***

The dependent variable, cybercrime victimization, was measured with the question "In the past three years, has someone committed a crime against you online?" with a *yes* or *no* response. If the participants answered *yes*, they were then asked to choose the type of crime committed from a dropdown list. Options in the dropdown list were: 1) Slander or defamation of your character, 2) Coercion or a threat of violence, 3) Identity theft, 4) Fraud, 5) Sexual harassment, and 6) Other, which? In case the participant chose option 6 they were asked to write the type of crime into a free text

box. The cut-off of three years was selected because of its use in previous victimization studies and because online victimization is a relatively rare life event (Kaakinen et al., 2018; Näsi et al., 2015).

A total of eight independent variables from our data were selected including both theoretical and control measures. Three components of RAT included exposure to a motivated offender, target suitability, and guardianship. We are using similar measures for these components as previous studies (e.g. Marcum, 2008; Marcum et al., 2010; Näsi et al., 2016). Self-control was measured as the key concept from general theory of crime. Age and gender were used as control variables. All independent variables showed acceptable inter-item reliability. Descriptive statistics of independent variables and their reliability coefficients (Cronbach´s alpha) are introduced in Table 1.

(Table 1 around here)

**Exposure to motivated offender.** Exposure to motivated offenders was measured by creating two variables. The variable *Danger Sites* was created by using the question "How often do you use the following online sites and services." Options were "Dark web (for example: Tor, Freenet, I2P)," "Online casino sites or other sites by gambling companies," and "Online gambling forums or gambling communities." Each option had a response scale from 0 (*never*) to 3 (*daily*). The final danger sites scale ranged from 0 to 9. Social Media Sharing was created from questions "How often do you share content in social media" and "How often do you upload pictures of yourself into social media." The response scale was from 1 (*Less than once a year*) to 7 (*Daily*).

**Target suitability**. We measured target suitability using the Compulsive Internet Use Scale (CIUS; Meerkerk, Van Der Eijnden, Vermulst & Garretsen, 2009) and created a variable for *Offending Messaging*. The CIUS uses 14 items to measure

compulsive use of the Internet. The assumption behind CIUS is that a person is not addicted to the Internet itself but rather to particular social media services or other online activities, such as online gambling, which results in compulsive Internet use. Consequently, resulting in higher risk of getting victimized (Dihr, Chen & Nieminen, 2015; Griffiths, 2000). The response scale for CIUS ranged from 0 (*Never*) to 4 (*Very often*).

Aggressive behavior was measured by creating a variable called *Offending messaging* using the question "How often do you send messages in social media that offend or threaten other users?" The higher the participant scores, the higher the risk of being noticed as a suitable target by offenders. The response scale for *Offending messages* ranged from 1 (*Never*) to 7 (*Daily*).

**Absence of guardianship.** We treat the absence of guardianship as a lack of meaningful social relationships that is manifested in feelings of loneliness. This was measured using the Revised UCLA three-item Loneliness Scale (R-UCLA; Hughes, Waite, Hawkley & Cacioppo, 2004) which is used as a unidimensional measure of loneliness. R-UCLA scale has been used widely in multinational loneliness studies (De Jong Gierveld & Van Tilburg, 2010). The response scale ranged from 1 (*Rarely*) to 3 (*Often*).

**Self-Control.** Self-Control is a key concept in general theory of crime (Dussault, Brendgen, Vitaro, Wanner & Tremblay, 2011). Here, it was measured using the Eysenck Impulsiveness Scale (EIS; Eysenck & Eysenck, 1978). The scale is composed of five items. The response scale ranged between 0 and 5, with higher scores indicating higher level of impulsivity. One of the items ("Do you usually think carefully before doing anything?") was reverse coded prior to the analyses.

**Control factors.** We used the participants' gender (0 = male, 1 = female) and age as control factors. Age was treated as a continuous variable.

(Table 2 around here)

***Statistical techniques***

First, we calculated the percentage of respondents who reported to be targets of cybercrime at least once in the past three years. Descriptive findings in Table 1 include rates of cybercrime victimization for each country. We then examined the effect of the selected independent variables representing exposure to motivated offender, guardianship, and target suitability, on the probability of being a victim of cybercrime. We used logistic regression because of our dichotomous outcome variable. We were also interested in whether the impact of the independent variables was constant across the four countries.

For the mediation analysis, we used The Karlson–Holm–Breen (KHB) KHB method in Stata 15.1. This was conducted with the khb command (Kohler, Karlson & Holm, 2011). KHB is a decomposition method that solves issues related to comparison of nested nonlinear models (Mood, 2010) and, thus, is able to estimate mediation effects that are robust to rescaling bias (Karlson, Holm & Breen, 2012). KHB gives an estimation of variance explained by mediator Z in nonlinear models. It also solves issues arising especially in comparison of nonlinear models (Mood, 2010). Our models included all three mediators at the same time and age and gender as controls. We report how much of the total effect is explained by the mediators. We also bootstrapped the KHB models with 10,000 replications and provided total mediating effects for each country**.**

**Results**

Cybercrime victimization was substantial in each of the studied countries, with 4.3 to 7.9 percent of the respondents reporting being a target. The rates of cybercrime victimization (Table 1) were highest in Finland and lowest in South Korea. In the U.S., 85 (7.0%) participants reported cyber victimization, while the same frequency was 95 in Finland (7.8%), 87 in Spain (7.2%), and 51 (4.3%) in South Korea. All four countries combined and both genders considered, the most common forms of cybercrime faced by the victims were slander or defamation of one's character and coercion or a threat of violence. Sexual harassment was the least common form of reported cybercrime.

The most common reported form of cybercrime among female participants was slander or defamation of one's character followed by sexual harassment, while the least common was fraud, except in Finland. In Finland, fraud was the most common form of crime among female victims followed by slander or defamation of one's character and sexual harassment. The most common form of cybercrime faced by male respondents was slander or defamation of one's character, except in the U.S., where coercion or a threat of violence was the most common form of cybercrime. Table 3 reports the unstandardized regression weights (B), their standard errors, odds ratios (OR) and p-values. Also, chi-square ($\chi^2$) log likelihood coefficients are presented for each model with the pseudo-coefficients of the determination (Nagelkerke Pseudo $R^2$).

(Table 3 around here)

Logistic regression analysis revealed that the participants who reported using danger sites more often also had a higher risk of being cyber victimized (Table 3). This finding was consistent in all four countries (U.S. OR = 1.26, $p < 0.001$, Finland OR = 1.168, $p < 0.05$, Spain OR = 1.181, $p < 0.01$, South Korea OR = 1.206, $p < 0.05$). Other variables based on RAT revealed mixed support as results varied between

countries. Sharing content online increased the risk of cyber victimization only in Spain (OR = 1.167, $p < 0.001$) and sending offending messages only in South Korea (OR = 1.311, $p < 0.01$). Loneliness increased the risk of victimization in Finland (OR = 1.149, $p < 0.05$) and Spain (OR = 1.196, $p < 0.05$) but not in the U.S. or South Korea. Of the control variables, only older age was found to increase the risk of cyber victimization in the U.S. (OR = 1.081, $p < 0.05$). In the final logistic regression model, low self-control was associated with cybercrime victimization in the U.S. (OR = 1.179, $p < 0.05$), Finland (OR = 1.346, $p < 0.001$), and Spain (OR = 1.163, $p < 0.05$), but not in South Korea.

(Figure 1 around here)

Figure 1 reports how much of the total effect is explained by the mediators in the KHB analysis. Results showed that all of the three RAT-related factors mediated the relationship between impulsivity and cybercrime victimization very well in South Korea (from 19.12% to 23.03%) and reasonably well in Spain (from 10.95% to 14.27%). However, in the U.S., only exposure (17.58%) and suitability (12.05%) mediated the relationship between impulsivity and cybercrime victimization. In Finland, RAT-related factors did not mediate the relationship between impulsivity and cybercrime victimization (from 1.52% to 4.76%). We found that the mediating effect of all three RAT-related factors remained in the U.S. (9.4%, SE 2.5%, $p < .000$), Finland (3.4%, SE 1.2%, $p = .004$), Spain (10.4%, SE 2.7%, $p < .000$), and South Korea (10.1%, SE 2.4%, $p < .000$).

**Discussion**

Understanding the threats young people face while using the Internet and social media is vital in the fight against online crime. It is imperative to gain better

understanding of the factors associated with cybercrime victimization in an effort to reduce cyber victimization and provide increased safety and security online.

We took an approach in which we used RAT with its three key elements and expanded it with the core element of general theory of crime, namely low self-control, to study cybercrime victimization factors with well-balanced comparative cross-national data from four countries. General theory of crime utilizes notions from RAT and these two theories are considered consistent with one another as they have been integrated in previous crime victimization studies on conventional crime (e.g. Ngo & Paternoster, 2011; Ren et al., 2017; Stewart et al., 2004; Turanovic & Pratt, 2014).

The relationship between the variables associated with RAT and cybercrime victimization varied between the countries examined, as many of the variables failed to be significantly related to cybercrime victimization in every country. Exposure to motivated offender from RAT was the only factor throughout all four countries with statistical significance. This finding is similar with what Näsi and colleagues (2016) noted in their cross-national study on adults' online harassment victimization. Low self-control (i.e., impulsivity) failed to be statistically significant in South Korea. It is also important to note that compulsive Internet use was the only RAT associated variable which had no statistical significance in any of the countries in our study. The amount of variance accounted for (Nagelkerke Pseudo $R^2$) was moderate in Finland (0.099), but stronger in the U.S., Spain, and South Korea, varying between 0.128 and 0.167. The results suggest that our model is useable in a cross-national context, but future studies should pay more attention to the chosen RAT-related variables.

Young age, risk-driven lifestyle, and peer pressure are factors contributing to cyber victimization. In existing victimization and harassment studies, age has been a

statistically significant factor in explaining victimization: the younger the Internet user is the higher the risk of victimization (Näsi et al., 2016; Staksrud, Ólafsson & Livingstone, 2013). In our study, age was a significant contributor only in the U.S. This could be because of changes in the way the Internet is being used today by adolescents. Younger people have been more active users of the Internet and social media (Näsi et al., 2016), but it could be that among the 15 to 25 year old age group, the Internet is being used in similar ways and equally actively regardless of the age of the respondent. In our study, we did not ask the participants if they have changed the way they use the Internet, and how they utilized it in the past. Future studies could be constructed to study possible changes and the meaning of these changes for cyber victimization.

In existing online harassment studies, women tend to be more commonly the victims of sexual harassment (e.g., Duggan, 2014; Näsi et al., 2016). In our study, the most common type of cybercrime female respondents experienced was slander or defamation of one's character, except in Finland, where fraud was the most common crime. This raises questions if online sexual harassment has truly decreased or is sexual harassment so common on the Internet that it is no longer considered a criminal act, but rather something that is simply part of online communities. Either way, this possible change in crime types should be taken into consideration in future studies.

The RAT-related factors, exposure to motivated offender, target suitability, and absence of guardianship partially mediated the relationship between low self-control and cybercrime victimization. In previous studies, a similar mediating role of risky lifestyles has been noted especially in terms of conventional or "real-life" crimes (e.g., Ren et al., 2017; Stewart et al., 2004). Under this theoretical model, low self-control leads to exposure, suitability, and lack of guardianship, and further to cybercrime victimization. However, the findings of our study could indeed suggest that

the significance of self-control should be reviewed in future studies as its effects are mediated by RAT-related factors.

**Limitations**

The foremost strength of our study is the comparative data samples from four different countries covering three different continents. They allowed for the comprehensive examination of cybercrime victimization in a multi-national context using two established criminological theories from a social psychological perspective.

Given that our analyses were based on cross-national survey data, the participant responses could contain a variety of biases in terms of criminality classification. In addition, the possible participants' (un)willingness to report having been cybercrime victimized should be noted since willingness to report victimization could vary between countries and cultures. However, the self-report approach to victimization research has been utilized in previous studies and yielded meaningful results (Bossler & Holt, 2010; Kaakinen et al., 2018; Oksanen & Keipi, 2013; Reyns et al., 2011). The cross-sectional design of our study makes it possible to test the mediation model only on a theoretical basis. Our theoretical approach should be tested further in future longitudinal studies.

**Conclusions and implications**

Despite the usefulness of RAT, other aspects, such as self-control should be taken into consideration when exploring cybercrime victimization. This study demonstrates the need to expand and test established theories of crime and cybercrime victimization cross-nationally in order to better understand the global phenomenon more comprehensively.

We included four different countries from across three different continents in our study. All four countries can be considered as societies with high Internet and

social media penetration percentages (Internet World Stats, 2019; Statista 2019). At the same time, it can be argued the studied countries differ substantially from each other, especially when it comes to cultural and societal factors. These differences between the studied countries could explain the differences observed in our final results. Our recommendation is that future studies should continue analyzing cross-national differences in cybercrime victimization. Studies should consider different cultural and societal factors, such as to what extent people in different cultures are thought to control their impulses, and how parents follow, limit, or control adolescents' Internet use. Our dataset of four countries (only four level-2 units) limited our ability to run multilevel assessment to study country level variance. We recommend this to be a research area for future studies.

Based on the results of our study, several general recommendations and guidelines can be made for cybercrime victimization situations. First, more information and services about cybercrime and cybercrime prevention should be targeted and made available for parents. Without cybercrime awareness and proper training, the prevention of cyber victimization will not be successful. As long as adults or other family members fail to provide aid for adolescents in time of a problem, no meaningful impact can be made.

Second, the more adolescents and young adults use social media services, the higher their risk of being victimized. This does not mean that disconnecting them from the Internet or social media services is the solution. This could disconnect adolescents from supportive peer groups and harm their social life. Instead, parents should negotiate and delimit the amount of time adolescents spend online and observe what their children share over the Internet and, importantly, with whom.

Third, parents, schoolteachers, policy makers, and social media administrators should encourage children to share their online experiences with adults, especially if children face cyber harassment or cybercrime. They should also be encouraged to report possible cybercrime experiences to the local law enforcement agencies. Lastly, as children start using the Internet and social media at an early age, responsible online behavior should be promoted as early as possible, just like parents normally would do in the physical world.

**References**


Akers, R. L. & Lee, G. (1999). Age, social learning, and social bonding in adolescent substance use. *Deviant Behavior*, *20*(1), 1–25. https://doi.org/10.1080/016396299266579

Baumeister, R.F. & Leary, M.R. (1995). The need to belong: desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin*, 117(3), 497–529.

Baumeister, R.F. & Heatherton, T.F. (1996). Self-regulation failure: An overview. *Psychological inquiry*, 7(1), 1–15. https://doi.org/10.1207/s15327965pli0701_1

Bossler, Adam, Thomas Holt. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, 3(1), 400-420

Bossler, A.M. & Holt, T.J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38(3), 227–236. https://doi.org/10.1016/j.jcrimjus.2010.03.001

Cohen, L.E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588–608. https://doi.org/10.2307/2094589

De Jong Gierveld, J. & Van Tilburg T. (2010). The De Jong Gierveld short scales for emotional and social loneliness: tested on data from 7 countries in the UN generations and gender surveys. *European Journal of Ageing*, 7(2), 121–130. https://doi.org/10.1007/s10433-010-0144-6

Dihr, A., Chen, S. & Nieminen, M. (2015). A repeat cross-sectional analysis of the psychometric properties of the Compulsive Internet Use Scale (CIUS) with adolescents from public and private schools. *Computers & Education*, 86, 172–181. https://doi.org/10.1016/j.compedu.2015.03.011

Duggan M. (2014). Online harassment. www.pewinternet.org/2014/10/22/online-harassment.

Dussault, F., Brendgen, M., Vitaro, F., Wanner, B. & Tremblay, R.E. (2011). Longitudinal links between impulsivity, gambling problems and depressive symptoms: A transactional model from adolescence to early adulthood. *Journal of Child Psychology and Psychiatry*, 52(2), 130–138. https://doi.org/10.1111/j.1469-7610.2010.02313.x

Ellonen, N. & Salmi, V. (2011). Poly-Victimization as a Life Condition: Correlates of Poly-Victimization among Finnish Children. *Journal of Scandinavian Studies in Criminology & Crime Prevention*, 12(1), 20–44. https://doi.org/10.1080/14043858.2011.561621

Eysenck, S.B.G. & Eysenck, H.J. (1978). Impulsiveness and venturesomeness: Their position in a dimensional system of personality description. *Psychological Reports*, 43, 1247–1255. https://doi.org/10.2466/pr0.1978.43.3f.1247

Felson, M. (2016). Routine Activity Approach. In: R. Wortley & M. Townsley (eds.). *Environmental Criminology and Crime Analysis*. (pp. 87–97) New York: Routledge.

Finkelhor, D., Ormrod, R., Turner, H. & Hamby, S. (2005). Measuring Poly-Victimization Using the Juvenile Victimization Questionnaire. *Child Abuse & Neglect*, 29, 1297–1312. https://doi.org/10.1016/j.chiabu.2005.06.005

Gañán, C.H., Ciere, M. & van Eeten, M. (2017). Beyond the pretty penny: the Economic Impact of Cybercrime. *Proceedings of the 2017 New Security Paradigms Workshop,* 35–45. https://doi.org/10.1145/3171533.3171535.

Gonzales, A. & Hancock, J. (2010). Mirror, Mirror on My Facebook Wall: Effects of Exposure to Facebook on Self-Esteem. *Cyberpsychology, behavior and social networking*, 14, 79-83. https://doi.org/10.1089/cyber.2009.0411.

Gottfredson, M.R. & Hirschi, T. (1990). *A general theory of crime*. Stanford: Stanford University Press.

Griffiths, M. (2000). Excessive Internet Use: Implications for Sexual Behavior. *CyberPsychology & Behavior*, 3(4). https://doi.org/10.1089/109493100420151

Griffiths, G., Norris, G. (2020). Explaining the crime drop: contributions to declining crime rates from youth cohorts since 2005. *Crime Law Soc Change*, 73, 25–53. https://doi.org/10.1007/s10611-019-09846-5

Hay, C., Meldrum, R. & Mann, K. (2010). Traditional bullying, cyber bullying, and deviance: A general strain theory approach. *Journal of Contemporary Criminal Justice*, 26(2), 130–147. https://doi.org/10.1177/1043986209359557

Hay C. & Ray K. (2019). General Strain Theory and Cybercrime. In: T. Holt & A. Bossler (eds.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. (pp. 1–19) Palgrave Macmillan, Cham

Hofmann, W., Luhmann, M., Fisher, R.R., Vohs, K.D. & Baumeister, R.F. (2013). Yes, But Are They Happy? Effects of Trait Self-Control on Affective Well-Being and Life Satisfaction. *Journal of Personality,* 82(4), 265–353. https://doi.org/10.1111/jopy.12050

Holt, T.J. & Bossler, A.M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behaviour*, 30(1). https://doi.org/10.1080/01639620701876577.

Holt, T. J., Leukfeldt, R. & Van De Weijer, S. (2020). An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites. *Criminal Justice and Behavior*. https://doi.org/10.1177/0093854819900322

Hughes, M.E., Waite, L.J., Hawkley, L.C. & Cacioppo, J.T. (2004). A Short Scale for Measuring Loneliness in Large Surveys: Results from Two Population-based Studies. *Research on aging*, 26(6), 655–672. https://doi.org/10.1177/0164027504268574

Internet Live Stat (2019). Internet users. http://www.internetlivestats.com/internet-users/#sources

Internet World Stats (2019). World Internet Users and 2019 Population Stats. https://www.internetworldstats.com/stats.htm

Kaakinen, M., Keipi, T., Räsänen, P. & Oksanen, A. (2018). Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 129–137. https://doi.org/10.1089/cyber.2016.0728

Karlsson, K. B. & Holm, A. (2011). Decomposing primary and secondary effects: A new decomposition method. *Research in Stratification and Social Mobility* 29, 221–237. https://doi.org/10.1016/j.rssm.2010.12.005

Kerstens, J. & Jansen, J. (2016). The Victim–Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth's On-Line Victimization and Perpetration. *Deviant Behavior* 37(5), 585–600. https://doi.org/10.1080/01639625.2015.1060796.

Kranenbarg, M.W., Holt, T.J. & van Gelder, J-L. (2019). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. *Deviant Behavior*, 40(1), 40–55. https://doi.org/10.1080/01639625.2017.1411030

Kivivuori, J., Aaltonen, M., Näsi, M., Suonpää, K. & Danielsson, P. (2018). *Kriminologia. Rikollisuus ja kontrolli muuttuvassa yhteiskunnassa*. Helsinki: Gaudeamus.

Kim, J., Larose, R. & Peng, W. (2009). Loneliness as the cause and the effect of problematic internet use: the relationship between internet use and psychological well-being. *Cyberpsychology & Behavior*, 12(4), 451–455. https://doi.org/10.1089/cpb.2008.0327

Kohler, U., Karlson, K. B. & Holm, A. (2011). Comparing coefficients of nested nonlinear probability models. *The Stata Journal,* 11(3), 420–438.

Kulig, T.C., Pratt, T.C., Cullen, F.T., Chouhy, C. & Unnever, J.D. (2017). Explaining Bullying Victimization: Assessing the Generality of the Low Self-Control/Risky Lifestyle Model, Victims & Offenders, 12(6), 891-912. https://doi.org/10.1080/15564886.2017.1307297

Leukfeldt, E.R. (2014). Phishing for suitable targets in the Netherlands: routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking,* 2014(17), 551–555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E.R. & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior,* 37(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Marcum, C.D. (2008). Identifying Potential Factors of Adolescent Online Victimization. *International Journal of Cyber Criminology*, 2(2), 346–367.

Marcum, C.D., Higgins, G.E. & Ricketts, M.L. (2010). Potential factors of online victimization of youth: an examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, 31, 381–410. doi.org/10.1080/01639620903004903.

Martinez, N.M., Lee, Y., Eck, J.E. & O, S. (2017). Ravenous wolves revisited: a systematic review of offending concentration. *Crime Science*, 6(10). https://doi.org/10.1186/s40163-017-0072-2.

Mason, K.L. (2008). Cyberbullying: A preliminary assessment for school personnel. *Psychology in the Schools*, 45(4), 323–348. https://doi.org/10.1002/pits.20301

Meerkerk, G.-J., Van Den Eijnden, R.J.J.M., Vermulst, A.A. & Garretsen, H.F.L. (2009). The Compulsive Internet Use Scale (CIUS): Some Psychometric Properties. *CyberPsychology & Behavior*, 12(1). https://doi.org/10.1089/cpb.2008.0181

Meško, G. (2018). On some aspects of cybercrime and cybervictimization. *European Journal of Crime, Criminal Law, and Criminal Justice*, 26(3). https://doi.org/10.1163/15718174-02603006

Mood, C. (2010). Logistic Regression: Why We Cannot Do What We Think We Can Do, and What We Can Do About It. *European Sociological Review*, 26(1), 67–82. https://doi.org/10.1093/esr/jcp006.

Ngo, F.T. & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, 5(1), 773–793.

Näsi, M., Oksanen, A., Keipi, T. & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 16(2), 203-210. https://doi.org/10.1080/14043858.2015.1046640.

Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T. & Oksanen, A. (2016). Do routine activities help predict young adults' online harassment: A multi-nation study.

*Criminology & Criminal Justice*, 1–15. https://doi.org/10.1177/1748895816679866.
Perlman, D. & Peplau, A. (1981). Toward a Social Psychology of Loneliness. In: S. Duck & R. Gilmour (eds.) *Personal Relationship in Disorder*. (pp. 31–56). London: Academic Press. https://doi.org/10.4236/psych.2019.1015137
Office for National Statistics (2015). Improving Crime Statistics in England and Wales. *Crime Statistics, Year Ending June 2015 Release*. http://webarchive.nationalarchives.gov.uk/20160105160709/ http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html
Oksanen, A. & Keipi, T. (2013). Young People as Victims of Crime on the Internet: A Population-based Study in Finland. *Vulnerable Children & Youth Studies*, 8(4), 298–309. https://doi.org/10.1080/17450128.2012.752119
Oksanen, A., Sirola, A., Savolainen, I. & Kaakinen, M. (2019). Gambling patterns and associated risk and protective factors among Finnish young people. *Nordic Studies on Alcohol and Drugs,* 36(2), 161–176. https://doi.org/10.1177/1455072518779657
Pratt, T. C. (2016). A self-control/life-course theory of criminal behavior. *European Journal of Criminology*, 13, 129–146. https://doi.org/10.1177/1477370815587771
Ren, L., He, N., Zhao, R. & Zhang, H. (2017). Self-Control, Risky Lifestyles, and Victimization. A Study With a Sample of Chinese School Youth. *Criminal justice and behavior*, 44(5), 695–716. https://doi.org/10.1177/0093854816674758
Reyns, B.W. (2011). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, 50(2), 216–238. https://doi.org/10.1177/0022427811425539
Reyns, B.W., Henson, B. & Fisher, B.S. (2011). Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, 38(1149), 1148–1169. https://doi.org/10.1177/0093854811421448.
Reyns, B.W., Henson, B. & Fisher, B.S. (2014). Digital Deviance: Low Self-Control and Opportunity as Explanations of Sexting Among College Students. *Sociological Spectrum, 34*(3), 273–292. https://doi.org/10.1080/02732173.2014.895642
Reisig, M.D. & Golladay, K.A. (2019). Violent victimization and low self-control: The mediating effect of risky lifestyles. *Violence and Victims,* 34(1), 157–174. https://doi.org/10.1891/0886-6708.34.1.157
Saini, H., Rao, Y.S. & Panda, T.C. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA)*, 2(2), 202–209. http://www.academia.edu/download/38524184/10.1.1.417.1369.pdf
Schreck, C.J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly*,16, 633–654. https://doi.org/10.1080/07418829900094291
Schreck, C.J., Wright, R.A. & Miller, J.M. (2002). A study of individual and situational antecedents of violent victimization. *Justice Quarterly,* 19, 159–80. https://doi.org/10.1080/07418820200095201
Seidman, G. (2013). Self-presentation and belonging on Facebook: How personality influences social media use and motivations. *Personality and Individual Differences*, 54, 402–407. https://doi.org/10.1016/j.paid.2012.10.009.

Staksrud, E., Ólafsson, K. & Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior*, 29(1), 40–50. https://doi.org/10.1016/j.chb.2012.05.026

Statista (2019). Number of social media users worldwide from 2010 to 2021 https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Stewart, E.A., Elifson, K.W. & Sterk, C.E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. J*ustice Quarterly*, 21(1), 159–181. https://doi.org/10.1080/07418820400095771

Tagney, J.P., Boone, A.L. & Baumeister, R.F. (2018). High self- control predicts good adjustment, less pathology, better grades, and interpersonal success. In R. F. Baumeister (ed.) *Self- Regulation and Self- Control. Selected works of Roy F. Baumeister.* (pp. 173–212). London: Routledge.

Tcherni, M., Davies, A., Lopes, G. & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?. *Justice Quarterly,* 33(5), 890–911. https://doi.org/10.1080/07418825.2014.994658

Turanovic, J.J. & Pratt, T.C. (2014). "Can't Stop, Won't Stop": Self-Control, Risky Lifestyles, and Repeat Victimization. *Journal of Quantitative Criminology*, 30(1), 29–56. https://doi.org/10.1007/s10940-012-9188-4

Warr, M. (1993). Age, peers, and delinquency. *Criminology*, *31*(1), 17-40. https://doi.org/10.1111/j.1745-9125.1993.tb01120.x

White, J.L., Moffitt, T.E., Caspi, A., Bartusch, D.J., Needles, D.J. & Stouthamer-Loeber, M. (1994). Measuring impulsivity and examining its relationship to delinquency. *Journal of abnormal psychology*, 103(2), 192–205. https://doi.org/10.1037//0021-843x.103.2.192

Wigderson, S. & Lynch, M. (2013). Cyber- and traditional peer victimization: Unique relationships with adolescent well-being. *Psychology of Violence*, 3(4), 297-309. http://doi.org/10.1037/a0033657

Yar, M. (2005). The Novelty of 'Cybercrime'. An Assessment in Light of Routine Activity Theory. *European journal of Criminology*, 2(4), 407–427. http://doi.org/10.1177/147737080556056

Yar M (2013). Cybercrime and Society. London: SAGE

Yen, J., Ko, C., Yen, C., Chen, S., Chung, W. & Chen, C. (2008). Psychiatric symptoms in adolescents with internet addiction: comparison with substance use. *Psychiatry and Clinical Neurosciences*, 62, 9–16. https://doi.org/10.1111/j.1440-1819.2007.01770.x

Table 1.

Descriptive statistics. Categorical variables are presented as frequencies (*n*) and relational proportions (*%*). Continuous variables are presented as means (*M*), standard deviations (*SD*) and Cronbach's alphas ($\alpha$).

| | **United States** | | | | **Finland** | | | | **Spain** | | | | **South Korea** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *M* | *SD* | Range | α | *M* | *SD* | Range | α | *M* | *SD* | Range | α | *M* | *SD* | Range | α |
| Danger Sites | 0.80 | 1.79 | 0–9 | 0.863 | 0.93 | 1.37 | 0–9 | 0.703 | 1.10 | 1.90 | 0–9 | 0.842 | 0.43 | 1.30 | 0–9 | 0.852 |
| Social Media Sharing | 7.37 | 3.62 | 0–14 | 0.762 | 5.25 | 3.08 | 0–14 | 0.764 | 7.60 | 3.44 | 0–14 | 0.752 | 4.73 | 3.36 | 0–14 | 0.717 |
| Compulsive Internet Use | 21.73 | 13.54 | 0–56 | 0.948 | 18.79 | 11.13 | 0–56 | 0.929 | 22.18 | 12.66 | 0–56 | 0.938 | 23.14 | 12.81 | 0–56 | 0.953 |
| Offending Messaging | 1.74 | 2.23 | 0–7 | - | 0.58 | 1.31 | 0–7 | - | 1.55 | 2.16 | 0–7 | - | 0.90 | 1.65 | 0–7 | - |
| Loneliness | 5.52 | 1.86 | 3–9 | 0.821 | 5.53 | 1.78 | 3–9 | 0.830 | 5.11 | 1.77 | 3–9 | 0.809 | 5.23 | 1.73 | 3–9 | 0.843 |
| Impulsivity | 1.90 | 1.61 | 0–5 | 0.685 | 1.96 | 1.69 | 0–5 | 0.745 | 2.05 | 1.59 | 0–5 | 0.665 | 1.56 | 1.47 | 0–5 | 0.631 |
| Age | 20.05 | 3.19 | 15–25 | - | 21.29 | 2.85 | 15–25 | - | 20.07 | 3.16 | 15–25 | - | 20.61 | 3.24 | 15–25 | - |
| *Cat.variables* | coding | *n* | % | | | *n* | % | | | *n* | % | | | *n* | % | |
| Cybercrime victim | Yes | 85 | 7.01 | | | 95 | 7.92 | | | 87 | 7.18 | | | 51 | 4.28 | |
| | No | 1127 | 93.0 | | | 1105 | 92.1 | | | 1125 | 92.8 | | | 1141 | 95.7 | |
| Gender | Male | 604 | 49.83 | | | 600 | 50 | | | 621 | 51.24 | | | 591 | 49.58 | |
| | Female | 608 | 50.17 | | | 600 | 50 | | | 591 | 48.76 | | | 601 | 50.42 | |

Table 2.

Zero-order Correlation Matrix. Correlated variable = cybercrime victimization.

| *Variables* | *United States* $N = 1212$ | *Finland* $N = 1200$ | *Spain* $N = 1212$ | *South Korea* $N = 1192$ |
|---|---|---|---|---|
| Danger Sites | 0.244** | 0.117** | 0.225** | 0.231** |
| Social Media Sharing | 0.059* | 0.041 | 0.171** | 0.113** |
| Compulsive Internet Use | 0.122** | 0.092** | 0.155** | 0.120 |
| Offending Messaging | 0.129** | 0.115** | 0.158** | 0.212 |
| Loneliness | 0.073* | 0.072* | 0.135** | 0.099** |
| Impulsivity | 0.109** | 0.115** | 0.103** | 0.061* |
| Gender | 0.062* | -0.052 | 0.004 | -0.031 |
| Age | 0.095** | -0.031 | 0.091** | -0.022 |

* $p < 0.05$. ** $p < 0.01$.

Table 3.

Logistic Regression Country Tables for Cybercrime Victimization, by type of routine activity and low self-control.

| | *United States* | | | *Finland* | | | *Spain* | | | *South Korea* | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Variables* | B | SE | OR | B | SE | OR | B | SE | OR | B | SE | OR |
| *Control Variables* | | | | | | | | | | | | |
| Gender | -0.132 | 0.253 | 0.876 | -0.274 | 0.251 | 0.760 | 0.205 | 0.243 | 1.227 | -0.143 | 0.309 | 0.866 |
| Age | 0.077* | 0.039 | 1.081 | -0.028 | 0.040 | 0.972 | 0.077 | 0.040 | 1.080 | -0.016 | 0.046 | 0.984 |
| *Exposure* | | | | | | | | | | | | |
| Social Media Use | 0.231*** | 0.052 | 1.260 | 0.155* | 0.069 | 1.168 | 0.167** | 0.058 | 1.181 | 0.187* | 0.078 | 1.206 |
| Social Media Sharing | -0.015 | 0.039 | 0.985 | -0.003 | 0.038 | 0.997 | 0.155*** | 0.043 | 1.167 | -0.013 | 0.056 | 0.987 |
| *Suitability* | | | | | | | | | | | | |
| Compulsive Internet Use | 0.013 | 0.011 | 1.013 | 0.015 | 0.010 | 1.015 | 0.003 | 0.012 | 1.003 | 0.023 | 0.014 | 1.023 |
| Offending Messaging | 0.043 | 0.060 | 1.043 | 0.092 | 0.074 | 1.097 | 0.043 | 0.060 | 1.044 | 0.271** | 0.091 | 1.311 |
| *Guardianship* | | | | | | | | | | | | |
| Loneliness | 0.039 | 0.072 | 1.039 | 0.139* | 0.065 | 1.149 | 0.179* | 0.073 | 1.196 | 0.118 | 0.097 | 1.125 |
| *Low Self-Control* | | | | | | | | | | | | |
| Impulsivity | 0.164* | 0.079 | 1.179 | 0.297*** | 0.068 | 1.346 | 0.151* | 0.077 | 1.163 | 0.030 | 0.105 | 1.030 |
| | | | | | | | | | | | | |
| Constant | -5.158*** | 0.969 | | -3.496*** | 0.993 | | -7.568*** | 1.068 | | -4.390*** | 1.165 | |
| Model $\chi^2$ | 63.617*** | | | 51.361*** | | | 84.486*** | | | 55.230*** | | |
| Nagelkerke $R^2$ | 0.128 | | | 0.099 | | | 0.167 | | | 0.152 | | |

* $p < 0.05$. ** $p < 0.01$. *** $p < 0.001$.
Coefficients (B), Standard errors (SE)

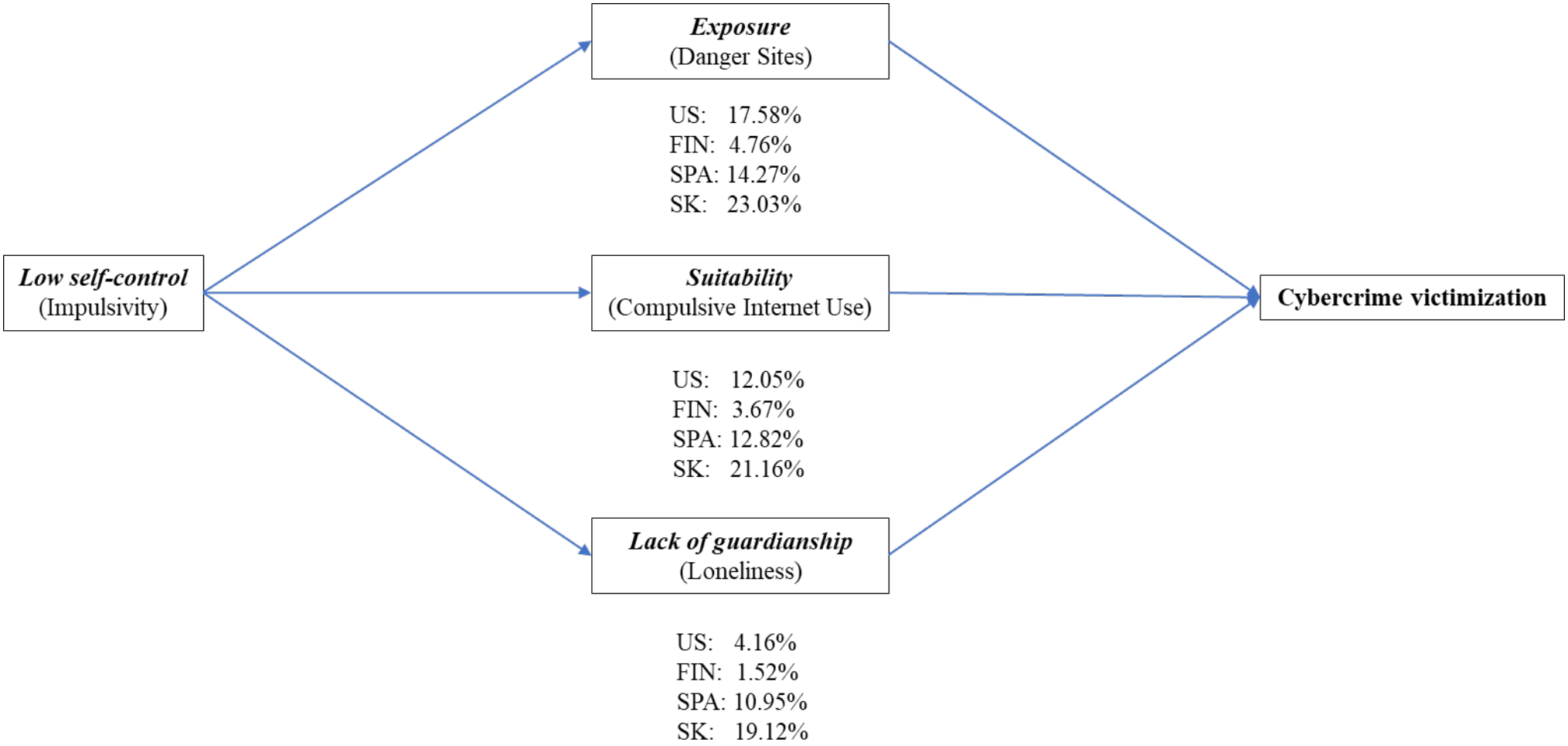


Figure 1.

The Relation Between Low Self-control and Cybercrime Victimization Mediated by RAT-related Factors.