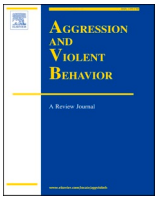
Aggression and Violent Behavior 70 (2023) 101836

Contents lists available at ScienceDirect

Aggression and Violent Behavior

journal homepage: www.elsevier.com/locate/aggviobeh



Risk factors for juvenile cybercrime: A meta-analytic review

Inge B. Wissink [a,*], Joyce C.A. Standaert [b], Geert Jan J.M. Stams [b], Jessica J. Asscher [a], Mark Assink [b]

[a] Forensic Child and Youth Care Sciences, Social and Behavioural Sciences: Education and Pedagogy, Utrecht University, Heidelberglaan 1, 3508 TC Utrecht, the Netherlands

[b] Research Institute of Child Development and Education, University of Amsterdam, Nieuwe Achtergracht 127, 1018 WS Amsterdam, the Netherlands

ARTICLE INFO

Keywords:
Cybercrime
Cyberstalking
Hacking
Sexting
Risk factors
Meta-analysis

ABSTRACT

So far, most meta-analyses and reviews on juvenile crime risk factors focused on risk factors for traditional crimes. It is unknown, though, whether these risk factors are also relevant for the explanation of cybercrime perpetration. This meta-analytic review aimed to identify risk factors for cyberstalking, hacking, and sexting perpetrated by juveniles. A literature search yielded 48 articles (24 for cyberstalking, 15 for sexting, and 10 for hacking) that produced 903 effect sizes (306 for cyberstalking, 61 for sexting, and 536 for hacking). The results showed similarities, but also differences in risk factors for the three types of cybercrime. Overall, peer factors were found to be important for all three types (deviant peers for cyberstalking and hacking and peer pressure for sexting). Besides, for cyberstalking, previous online and offline perpetration and victimization were significant risk factors. Other small but significant effects for multiple cybercrime types were found for dark personality traits (for cyberstalking and sexting) and high computer preoccupation (for cyberstalking and hacking). Implications for (preventive) intervention are discussed, as well as the need for future research.

1. Risk factors for juvenile cybercrime: a meta-analytic review

Worldwide, there has been a clear rise of computer, smartphone, and internet use (Johnson, 2021). The COVID-pandemic forced us to have even more online contact with other people. But even before the pandemic, juveniles had already started to use a personal smartphone or computer more and more, and also at increasingly younger ages (Lee, 2018; Madden et al., 2013). These developments have great advantages, but also brought a higher urge for paying attention to associated challenges, such as how to deal with individuals who show unacceptable behavior or even commit offenses online (cybercrimes), and how to prevent such individuals from entering such a developmental path at all.

Most meta-analyses and reviews on juvenile crime have focused on risk factors for traditional (offline) crimes. It is unknown, though, whether these risk factors can also explain cybercrime perpetration. If unique risk factors are present in cybercrime perpetrators, this would mean that 'traditional' prevention and intervention programs might need to be adapted. An important question, therefore, is what variables can be identified as risk factors for cybercrime and how strong these risks are. This meta-analytic study is focused on answering that question.

Cybercrimes are often divided into cyber-dependent crimes and cyber-enabled crimes (Wall, 2015). Cyber-dependent crimes depend upon technology, meaning that the crime would not have existed without the technology. On the other hand, cyber-enabled crimes are traditional crimes that already existed before the cybertechnological developments, but they can now be performed at a larger scale and in a different form by using cybertechnology (Wall, 2015). In this meta-analytic study, hacking was examined as a form of cyber-dependent crime, whereas cyberstalking and sexting were examined as forms of cyber-enabled criminal behaviors.

Cybercrimes can have severe consequences for victims, such as post-traumatic stress disorder, trust issues, depression, anxiety, sleeping problems, and public availability of sensitive information (Bates, 2017; Dreßing et al., 2014; Furnell & Warren, 1999). Preventing (re)perpetration of cybercrime is therefore important. Information about risk factors is necessary to design effective prevention and intervention programs.

The three cybercrimes that are examined in this meta-analysis (cyberstalking, sexting, hacking) are considered to be illegal and prosecutable in most countries. However, the specific definitions of cyberstalking, sexting, and hacking may change in reaction to ongoing

* Corresponding author.
E-mail address: I.B.Wissink@uu.nl (I.B. Wissink).

https://doi.org/10.1016/j.avb.2023.101836
Received 18 April 2021; Received in revised form 22 February 2023; Accepted 18 March 2023
Available online 29 March 2023

developments. For cyberstalking, we choose to adopt the definition of Reyns et al. (2012), because it is based on the latest technological developments. Reyns et al. (2012) define cyberstalking as "the repeated pursuit of an individual using electronic or internet-capable devices" (p. 1). Cyberstalking refers to many different behaviors, such as sending or posting offensive or false messages, harassing, stealing and using the identity of the victim and acting to be somebody else (Bocij & McFarlane, 2002; Finn, 2004; Sheridan & Grant, 2007). Cyber dating abuse is often used interchangeably with cyberstalking and is commonly measured in the same manner as cyberstalking, although in the context of a dating relationship. Therefore, studies on cyber dating abuse were also included in the present review. Regarding sexting, only studies on the non-consensual creation and dissemination of sexual material were included (McGlynn & Rackley, 2017). As such, sexting includes forcing somebody to send a sext (i.e. a naked selfie taken for one's partner and not intended to be seen by anyone else) or video, or obtaining a picture or video secretly, as well as forwarding a video or picture without consent, after having it received from somebody else. In the literature, terminology to identify these behaviors is diverse, and includes: image-based sexual abuse, revenge porn, sexting behavior, forwarding images or videos without consent, non-consensual sharing, coercive sexting and sextortion (McGlynn & Rackley, 2017). Finally, hacking was defined as unauthorized trespassing or accessing other computers or networks (e.g., McGuire & Dowling, 2013). This concerns computer-to-computer hacking.

Even though rates of cyber deviant behavior are rising, not all types of deviant behavior have received a similar amount of attention in the literature. There are numerous studies on other forms of cyber deviant behavior, such as cyberbullying, illegal downloading, internet addiction, and gaming (e.g. Chen et al., 2017; Kuss & Griffiths, 2012). However, less is known about the less prevalent and more excessive (and prosecutable) cyber deviant behaviors, such as cyberstalking, sexting, and hacking. Thus, a meta-analysis of the risk factors for juvenile cyberstalking, sexting, and hacking is needed.

Andrews and Bonta (2010) identified the 'big four' or most important risk factors for criminal behavior: 'history of antisocial behavior', 'antisocial personality pattern', 'antisocial cognition', and 'antisocial associates'. Below, we shortly address these domains, the associated risk factors and theoretical backgrounds.

The 'history of antisocial behavior' risk domain includes prior offenses or prior antisocial activities. Juveniles might have been arrested in the past or may have committed multiple preceding offenses (Andrews & Bonta, 2010). The relevance of factors in this risk domain can be explained by several theories. Labelling theory explains that the labelling of (young) people who show rulebreaking behavior (i.e. primary deviance) as 'criminals' leads to societal reactions that make it hard for them to conform to the rules. 'Secondary deviance' is the reaction to (repeated) stigmatization (by police, justice, society) and refers to behavior that is in line with the assigned 'criminal' label. Other theories also pay attention to offenders' neuropsychological deficits that lead them to enter a criminal developmental path. For instance, with the dual taxanomy of offending behavior Moffitt (1993) described that there are two main types of offenders: an adolescence-limited group (who only exhibit antisocial behavior during adolescence) and a smaller group of life-course-persistent offenders (who show continuity in their antisocial behavior from early childhood into late adulthood). This continued antisocial behavior of the LCP group was considered to be the result of an interaction between neuropsychological deficits and difficult social environments and, throughout time, it would become more and more difficult to reverse such an antisocial developmental course. While this theory was later refined, it is still considered as one of the main 'life-course' theories.

In the 'antisocial personality pattern' risk domain several personality traits are included. For instance, low self-control is such a personality trait, which is expressed through impulsiveness, higher levels of risk-taking, not overseeing the consequences of one's actions and insensitivity. The general theory of crime explains that self-control prevents people from breaking rules and states that a low level of self-control is the result of ineffective parenting patterns in childhood (Gottfredson & Hirschi, 1990). When parents are emotionally unavailable or do not control their children in a constructive manner, children are at risk of developing low self-control and (cyber)crime can then be perceived as an easy and instant source of satisfaction. Other theories that explain the importance of factors in this 'antisocial personality pattern' domain are both low arousal and sensation seeking theory. These theories are based on the idea that some people have low arousal levels and are therefore less sensitive for punishment or negative consequences (low arousal theory) or seek sensation more than others (sensation seeking theory). Personality traits can also be described following the Big Five personality characteristics: extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience (Digman, 1990). Finally, some studies on traditional and cybercrime also examined dark personality traits, consisting of Machiavellianism, narcissism, psychopathy, and sadism (Paulhus, 2014).

The 'antisocial cognitions' risk domain comprises "attitudes, values, beliefs, rationalizations, and a personal identity that is favorable to crime" (Andrews & Bonta, 2010, p. 59). An example of a risk factor in this risk domain is low moral standards (Rogers, Seigfried, et al., 2006). For different cybercriminal behaviors it has indeed been found that perpetrators show relatively low internal moral values (Seigfried et al., 2008; Zezulka & Seigfried-Spellar, 2016) and low social moral values (Rogers, Smoak, et al., 2006). Kohlberg's theory of moral development explains how children develop morality and moral reasoning and the stages they go through.

The final 'antisocial associates' risk dimension of Andrews and Bonta (2010) encompasses that juveniles have peers that are involved in antisocial or criminal activities. Differential association theory of Sutherland (1947) explains that criminal behavior is learned behavior through interactions (contact) with criminal persons. In groups, not only criminal techniques, but also motives and rationalisations for criminal behavior are learned. Akers' (1998) social learning theory also states that criminal behavior is learned behavior. This theory emphasizes four mechanisms through which criminal behavior is learned: differential association, definitions (positive attitudes towards committing crime), imitation, and reinforcement. In Akers' theory the emphasis is more on the reinforcement or reward of deviant behavior (instead of on the contact).

Following these theoretical backgrounds, previous studies have already led to important insights regarding the role of various above-mentioned risk factors in explaining 'cybercrime' (see for example Boman & Freng, 2017; Holt et al., 2010; Navarro & Marcum, 2020; Nodeland & Morris, 2020). However, less is known about the importance of these risk factors (and the underlying theories) for the explanation of cyberstalking, sexting and hacking of young people specifically. The present study fills this gap in the literature.

1.1. The present study

In sum, this quantitative review meta-analytically summarizes the literature on the relations between several risk factors and juvenile perpetration of cyberstalking, sexting, and hacking. The first aim was to determine the relations between several different domains of risk factors and each of the three forms of youth cybercrime. The second aim was to examine how these relations were moderated by the general background variables gender, ethnicity, and educational stage.

2. Method

2.1. Eligibility criteria

Prior to the literature search, several inclusion and exclusion criteria were formulated. First, the mean age of the participants had to be

between 12 and 23 years. In the Netherlands, children from 12 years and older can be punished according to juvenile criminal law, while young people from 16 to 23 years old can be punished according to adolescent criminal law. Adolescent criminal law was especially developed following scientific insights that the adolescent brain is not fully developed until the age of 23 and that this must be taken into account in applying criminal law to criminal behavior of youngsters. Second, studies had to examine risk factors for perpetration of cybercrime meaning that studies on cybercrime victimization were not included. Third, solely articles reporting on risk factors for cyberstalking (including cyber dating abuse, digital dating abuse, and electronic intrusion), hacking, and/or sexting (including forwarding images or videos without consent, image-based sexual abuse, non-consensual dissemination, coercive sexting, revenge porn, and sextortion) were included. Articles on other cybercrimes, such as identity theft, illegal downloading, and online scams were excluded. However, if studies also examined cyberstalking, hacking and/or sexting, then these studies were included in our meta-analysis. Fourth, only studies that reported bivariate statistics were included. Therefore, studies had to report proportions, correlations, *t*-test results, chi-squared test results, bivariate odds ratios, or means and standard deviations. Multivariate statistics were excluded, as it is problematic to calculate standard errors and variances for multivariate statistics (Lipsey & Wilson, 2001). Fifth, studies had to be written in English or Dutch. Because of the novelty of the field, no restriction was set to the publication year of studies. Finally, for the same reason, both published studies in peer-reviewed journals as well as dissertations, government reports, and master theses were included.

2.2. Literature search

To search for relevant studies, four electronic databases were searched: ERIC, PsycINFO, Web of Science, and Google Scholar. The full syntax that was used to search these databases comprised combinations of keywords that refer to (1) the age of participants in the sample (mean age of participants must lie between 12 and 23 years), (2) cybercrime (and specifically cyberstalking, sexting, and hacking), and (3) study type (quantitative studies). The search procedure (see Appendix A for details) was performed until May 2019. Further, the reference lists of all included studies were scanned to identify additional studies that may have been missed in the electronic search. Finally, all included studies were entered in Google Scholar to determine whether additional studies could be identified by the 'cited by' function.

2.3. Selection of studies

Using the electronic databases, a total of 2126 eligible articles were found (175 from ERIC, 808 from PsycINFO, and 1143 from Web of Science). The Google Scholar search yielded one additional article. After removing duplicates 1626 articles were left. These articles were screened on title and abstract based on the inclusion- and exclusion criteria. To determine inter rater agreement, two authors blindly screened 154 articles and had an agreement of 96.1 %. Thus, the 154 articles were double-screened in the screening phase of deciding whether, based on title and abstract, the full-texts of the articles should be further examined for inclusion (in the eligibility phase). The large majority of the articles returned by our search string were excluded in this first screening phase because the studies focused on *adults* instead of adolescents (all abstracts are clear about whether the study focused on adults or adolescents, almost always confirmed by the mean age of respondents). Additionally, another substantial number of studies could not be included because the title and abstract made clear that the study focused on (risk factors for) cybercrime *victimization* instead of on (risk factors for) perpetration. Finally, titles and abstract sometimes made clear that studies only examined *composite variables* (such as 'online youth delinquent behavior', 'cyber deviance' or 'cyber offending') or other cybercrime variables as a dependent variable instead of the specific cybercriminal behaviors we were looking for (cyberstalking, hacking, and/or sexting).

Next, the full-text of the remaining 173 articles was examined to further decide on study eligibility. Initially, the strategy was to include studies focusing on cyber aggression, cyber harassment, trolling, online hate, and online insults, but this was changed as many of these behaviors – although deviant – could not be designated as severe deviant behavior. Therefore, only studies on cyberstalking were included (next to studies on sexting and hacking). Other reasons to exclude articles are reported in the flow diagram (Fig. 1). Finally, 48 articles were included in the meta-analysis, of which 24 reported on cyberstalking, 15 on sexting, and 10 on hacking (one article reported on both sexting and hacking). For an overview of the included studies and some of their study characteristics, see Appendix B.

2.4. Data coding

The 48 studies were coded with a coding sheet that was created in SPSS. After all studies were coded, separate SPSS files were created for cyberstalking, sexting, and hacking analyses. Ten percent of the included studies were double coded by two of the authors of this article, which showed an inter rater agreement of 99.9 %. Discrepancies in codings were discussed, after which all remaining studies were coded by the first author. In the coding procedure, study characteristics (e.g., year of publication), sample characteristics (e.g., percentage of males) and the effect size (e.g., correlation) were coded in accordance with guidelines and suggestions of Lipsey and Wilson (2001). A more elaborate description of all coded variables can be found in Appendix C.

Prior to analyzing the data, all coded risk factors were categorized into one of multiple created risk domains, which are groups of risk factors that are more or less similar in nature. For example, the factors parental education and parental income were categorized into the SES risk domain, as both factors refer to the socioeconomic status of sampled participants. Another example is the categorization of Machiavellianism, psychopathy, and narcissism into the single risk domain dark personality traits, as these three factors share that they refer to personality traits. In the end, thirty-five risk domains were identified for cyberstalking perpetration, 12 for sexting perpetration, and 22 for hacking perpetration. For each of these risk domains an average effect was estimated. For an overview of all risk domains and the risk factors categorized into these domains, see Appendix D.

Not all studies reported effect sizes in Pearson's *r* (i.e., the correlation between a risk factor and cybercrime perpetration). Other statistics that were reported were *t*-tests, chi-squared tests, and bivariate odds-ratios. Formulas of Lipsey and Wilson (2001) and Lenhard and Lenhard (2016) were used to transform these statistics into Pearson's *r*. One study reported Kendall's rank correlation, which was transformed to *r* with Walkers' (2003) formula. Some studies did not report the exact statistic of non-significant results. To prevent coding a null effect in these instances (i.e., $r = 0$), authors were mailed whenever possible. For nine of the cyberstalking and six of the sexting effect sizes it was not possible to retrieve an exact value and therefore a value of zero was coded as effect size. This approach is conservative and consequently leads to an underestimation of the real effect size (Lipsey & Wilson, 2001). However, it was the best approach at hand as we preferred a conservative approach above excluding effect sizes. For hacking such a null assignment was not necessary, since all non-significant results were reported in the studies. Some variables reported in the primary studies had to be recoded, because they were categorical (e.g., being male or female) or because they were examined as a protective factor instead of a risk factor (e.g., high self-control). In those cases, the effect sizes were inverted.

2.5. Statistical analyses

Before performing the main analyses, all continuous variables were

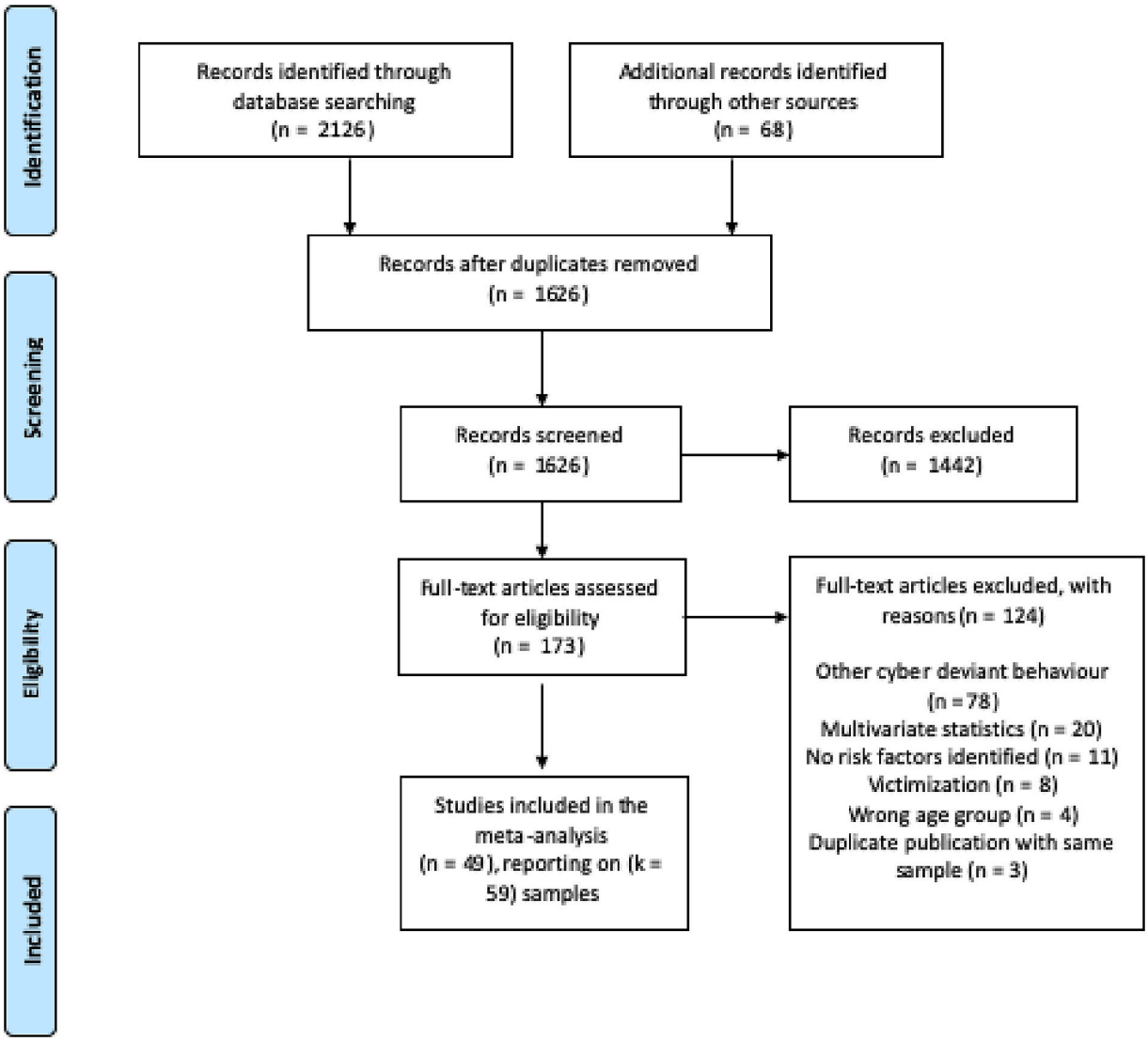


Fig. 1. PRISMA flow diagram cybercrime search.

mean centered, and for each dichotomous variable a dummy variable was created (e.g., published and not-published). Next, in each risk domain standard normal scores were calculated so that effect sizes could be checked for outliers. An effect size was considered to be an outlier when the *z*-value was above 3.29 or below −3.29 (Tabachnik & Fidell, 2013). No outliers were found in the risk domains, and therefore no effect size adjustments were done. Next, all Pearson's *r* correlations were transformed into Fisher's *z*-scores, because contrary to correlations, *z*-scores have a normal sampling distribution (Silver & Dunlap, 1987). For interpretability, the Fisher's *z* values were transformed back into Pearson's *r* correlation after the analyses were performed. Analyzing Fisher's *z*-values leads to less bias than synthesizing correlations without transforming them into Fisher's z values (Silver & Dunlap, 1987). Finally, the standard errors and variances were calculated (Lipsey & Wilson, 2001).

This meta-analysis uses a three-level random effects model that allows for the inclusion of multiple effect sizes per study. An important assumption in more traditional methods for meta-analysis is independence of effect sizes, which is violated when multiple effect sizes are extracted from the same study (Lipsey & Wilson, 2001). The three-level random effects model, however, deals with effect size dependency by specifying a three-level structure that models three types of variance (Assink & Wibbelink, 2016; Van den Noortgate et al., 2013). At level 1 of the three-level model the sampling variance is estimated. At level 2 the variance between effect sizes from the same study (within study variance) is estimated, and at level 3 the variance between studies is estimated. Van den Noortgate et al. (2013) illustrated in their simulation study that meta-analytic models with hierarchical multilevel structure as presented here can account for interdependency in both effect size and standard errors. To determine whether the within-study variance (at level 2) and/or the between-study variance (at level 3) were significant, two one-sided loglikelihood ratio tests were performed. When significant level 2 or level 3 variance was found within a risk domain, moderator analyses were conducted to examine whether any of the coded variables could explain this variance. As already mentioned, several sample characteristics were tested as moderators: the percentage of males in a primary study sample, the percentage of respondents with an ethnic majority background in a sample, educational stage, and specifically for cyberstalking the variable 'subtype of cyberstalking' was tested. This latter variable was coded and tested, as studies on both cyberstalking and cyber dating abuse were included. The (overall) effect of the risk domains were estimated for each of the three cybercrime forms separately (i.e. cyberstalking, sexting, and hacking). Bivariate moderator analyses were conducted within risk domains and separately for each of the three forms of cybercrime. All analyses were conducted in R Studio with the rma.mv function of the *metafor* package (Viechtbauer, 2010). The tutorial of Assink and Wibbelink (2016) was used in

conducting the analyses.

2.6. Publication bias

A common problem in meta-analyses is the 'file drawer problem' (Rosenthal, 1979). This refers to the problem that it is difficult to find the results of all research that has been conducted, as studies with non-significant results are often not accepted by journals, and are thus not publicly available. Whether or not publication bias may be a problem in a meta-analysis can be examined by inspecting funnel plots (Duval & Tweedie, 2000a). In a funnel plot, effect sizes are plotted against their standard errors which should result in a symmetric funnel-shaped plot. However, in case of publication bias, the funnel plot shows an asymmetric pattern, and a trim-and-fill analysis then produces a number of effect sizes that need to be imputed to restore the symmetry in the plot (Duval & Tweedie, 2000a). In this study, a trim-and-fill analysis was not performed due to the fact that many risk domains are based on a relatively small number of effect sizes. As the trim-and-fill analysis is not recommended when less than ten studies are synthesized (Macaskill et al., 2001), we decided to only visually inspect funnel plots. Based on this visual inspection, there were no strong indications for asymmetrical funnel plots, though no firm conclusions about the absence or presence of bias could be drawn given the relatively small number of studies that risk domains were based on. Funnel plots are displayed for all cyberstalking (Appendix E), sexting (Appendix F), and hacking (Appendix G) risk domains.

3. Results

3.1. Cyberstalking

For cyberstalking, a total of $N = 24$ articles examining $k = 29$ independent samples were included. The studies were published between 2010 and 2019 and conducted in the United States ($k = 18$), Canada ($k = 4$), the United Kingdom ($k = 1$), the Netherlands ($k = 1$), Turkey ($k = 1$), Portugal ($k = 1$), Belgium ($k = 1$), Australia ($k = 1$), and Spain ($k = 1$). In total, 306 effect sizes were extracted from these studies, with an average of 11.3 effect sizes per independent sample. The total sample size comprised $N = 20{,}368$ juveniles.

The overall association between all extracted risk factors and cyberstalking was significant and small in magnitude, $r = 0.174$, $p < .001$. As described in the Method section, all 306 studied risk factors were categorized into one of 35 risk domains (see Table 1) after which an overall effect for each of these domains was estimated. Seven factors that were extracted from the included studies (numbered 36 through 42 in Table 1) could not be classified into one of the created risk domains, due to their unique nature. Therefore, the effects of these single factors were based on information reported in the primary studies. The results showed that 15 of the 35 risk domains were significantly associated with cyberstalking perpetration. Cohen's (1988) criteria for interpreting correlations - that is ≥0.10, ≥0.30, and ≥0.50 for small, medium, and large correlations, respectively - were used for interpreting the strength of the overall effects of the risk domains. Strong risk domain effects were found for previous cybercrime perpetration ($r = 0.572$) and previous cyberstalking victimization ($r = 0.545$). Moderate effects were found for previous offline violence perpetration ($r = 0.395$), previous offline victimization ($r = 0.313$), and having deviant peers ($r = 0.300$). Small effects were found for dark personality traits ($r = 0.200$), substance abuse ($r = 0.159$), mental health problems ($r = 0.159$), attachment problems ($r = 0.146$), high computer preoccupation ($r = 0.137$), length of romantic relationship ($r = 0.133$), and negative gender norms and beliefs ($r = 0.121$). Finally, very small effects were found for risk behavior ($r = 0.096$), sexual risk behavior ($r = 0.096$), and a lack of social support ($r = 0.084$). Four of the seven individual risk factors were also significantly associated with cyberstalking with effect sizes ranging from $r = -0.060$ for insufficient social skills to $r = 0.870$ for having a history of digital dating abuse (see Table 1).

All cyberstalking risk domains were examined for effect size heterogeneity by determining the significance of the within-study variance (level 2) and between-study variance (level 3). If level 2 or level 3 variance was significant, moderator analyses were performed to search for variables that could explain this variance. The variables that were coded were tested as moderators in these analyses. The results of the moderator analyses are reported in Table 2. Eighteen domains showed significant level 2 and/or level 3 variance. To conduct meaningful moderator analyses, we only tested variables as moderators in risk domains that were based on at least five independent samples. This implied that moderator analyses were conducted for ten risk domains. Five significant moderating effects were found in three risk domains. The results showed that both the percentage of respondents with an ethnic majority background, $F(1, 8) = 17.402$, $p = .003$, and the subtype of cyberstalking, $F(1, 10) = 16.022$, $p = .003$, were significant moderators for the risk domain being male. The results indicated that the strength of the association between being male and cyberstalking perpetration increased when the percentage of juveniles with an ethnic majority background in the sample increased ($\beta = 0.239$). The effect of being male also increased when studies focused on cyberstalking (mean $r = 0.095$) compared to (the more specific) cyber dating abuse (mean $r = -0.077$), indicating that relatively more females perpetrated cyber dating abuse (compared to cyberstalking). Second, the percentage of males in the sample was found to be a significant moderator for the risk domain high computer preoccupation, $F(1, 14) = 6.754$, $p = .021$, $\beta = -313$. When the percentage of males in samples increased the effect of the domain high computer preoccupation increased. Third, both the percentage respondents with an ethnic majority background, $F(1, 7) = 7.152$, $p = .032$, $\beta = 0.190$, and educational stage, $F(1, 7) = 6.194$, $p = .003$, were significant moderators for the risk domain mental health problems. The effect of mental health problems increased when the percentage of participants with an ethnic majority background in samples increased. Further, in juveniles attending university the association between mental health problems and cyberstalking perpetration (mean $r = 0.202$) was stronger than in juveniles attending middle and high school (mean $r = 0.071$).

3.2. Sexting

For sexting, $N = 15$ articles were included examining $k = 19$ independent samples. The studies were published between 2012 and 2019, and were conducted in the United States ($k = 9$), Europe ($k = 6$), South Korea ($k = 1$), Australia ($k = 1$), Botswana ($k = 1$), and Canada ($k = 1$). Sixty-one effect sizes were extracted from the studies, with an average of 3.2 effect sizes per independent sample. The total sample consisted of $N = 16{,}816$ juveniles.

The overall association between all extracted risk factors and sexting was significant and small in magnitude, $r = 0.106$, $p < .001$. All 61 risk factors were categorized into one of twelve risk domains (see Table 3). The results revealed that the effect of only two of these risk domains was significant. That is, there was a small effect of dark personality traits ($r = 0.148$), and a very small effect of being male ($r = 0.071$). Several individual risk factors were not classified into a risk domain, as these factors appeared to be unique in nature. One of these individual risk factors was experiencing peer pressure, which showed to be significantly associated with sexting perpetration ($r = 0.490$) with a medium effect size. Further, a significant and small effect was found for having positive attitudes towards sexting ($r = 0.190$).

In all risk domains for sexting, heterogeneity in effect sizes was examined by testing the significance of the within-study variance (level 2) and the between-study variance (level 3). Three domains showed significant level 2 and/or level 3 variance, but as only one risk domain was based on at least five independent samples, moderator analyses were only conducted for one risk domain, which was being male. A moderating effect was found for educational stage on the effect of being

Table 1
Results of the overall mean effect sizes of risk domains for cyberstalking.

Risk domains	# studies	# ES	Mean Fisher's Z (SE)	95 % CI	Sig. mean Z (*p*)	Mean *r*	% var. at level 1	Level 2 variance	% var. at level 2	Level 3 variance	% var. at level 3
(1) Being male	11	12	−0.010 (0.032)	−0.082; 0.061	.759	−0.010	11.9	0.004	0.6	0.005*	87.6
(2) Being older	13	16	−0.003 (0.035)	−0.077; 0.070	.921	−0.003	12.2	0.000	0.6	0.013	87.3
(3) Being Caucasian	6	13	−0.015 (0.029)	−0.079; 0.049	.617	−0.015	12.3	0.010***	87.7	0.000	0.0
(4) Low self-control	2	3	0.133 (0.063)	−0.136; 0.402	.167	0.132	10.9	0.010***	89.1	0.000	0.0
(5) Being heterosexual	3	4	−0.030 (0.031)	−0.127; 0.067	.397	−0.030	40.4	0.000	0.0	0.002	59.6
(6) Higher school performance	6	10	−0.015 (0.034)	−0.092; 0.062	.672	−0.015	20.0	0.000	3.0	0.005	76.2
(7) Negative gender norms and beliefs	4	11	0.122 (0.018)	0.081; 0.163	<.001***	0.121	30.0	0.002**	67.8	0.000	2.3
(8) Agreeableness	1	2	−0.177 (0.027)	−0.519; 0.165	.096	−0.175	100.0	0.000	0.0	0.000	0.0
(9) Neuroticism	1	2	0.085 (0.035)	−0.363; 0.533	.250	0.085	58.3	0.001	41.7	0.000	0.0
(10) Openness	1	2	−0.060 (0.027)	−0.402; 0.282	.268	−0.060	100.0	0.000	0.0	0.000	0.0
(11) Dominance	2	2	0.230 (0.069)	−0.601; 1.01	.185	0.226	37.0	0.003	31.5	0.003	31.5
(12) Dark personality traits	5	16	0.203 (0.066)	0.063; 0.343	.008**	0.200	8.1	0.002*	7.8	0.020***	84.1
(13) High computer preoccupation	6	16	0.138 (0.055)	0.020; 0.255	.024*	0.137	10.2	0.007***	31.1	0.014*	58.8
(14) Substance abuse	4	7	0.160 (0.043)	0.055; 0.264	.010**	0.159	14.7	0.004*	48.8	0.003	36.5
(15) Being single	6	7	−0.091 (0.044)	−0.196; 0.014	.078	−0.091	12.4	0.000	0.0	0.010	87.6
(16) Previous cyberstalking victimization	6	10	0.611 (0.095)	0.397; 0.826	<.001***	0.545	1.4	0.036***	98.6	0.000	0.0
(17) Previous offline victimization	8	21	0.324 (0.065)	0.188; 0.459	<.001***	0.313	3.6	0.018***	41.7	0.024	54.6
(18) Previous offline violence perpetration	12	37	0.418 (0.077)	0.262; 0.574	<.001***	0.395	1.1	0.069***	60.1	0.044	38.8
(19) Previous cybercrime perpetration	6	7	0.651 (0.237)	072; 1.230	.033*	0.572	0.3	0.005	1.6	0.329	98.2
(20) Mental health problems	6	9	0.160 (0.038)	0.071; 0.248	.003**	0.159	23.6	0.004*	40.1	0.004	36.4
(21) Physical health problems	2	2	0.033 (0.034)	−0.404; 0.469	.517	0.033	89.9	0.000	5.1	0.000	5.1
(22) Length of romantic relationship	8	9	0.134 (0.043)	0.035; 0.232	.014*	0.133	12.9	0.002	11.5	0.010	75.6
(23) Risk behavior	2	7	0.096 (0.019)	0.046; 0.145	.004**	0.096	100.0	0.000	0.0	0.000	0.0
(24) Sexual risk behavior	3	6	0.096 (0.019)	0.046; 0.145	.004**	0.096	9.7	0.000**	90.3	0.000	0.0
(25) Ineffective coping strategies	2	6	0.071 (0.056)	−0.074; 0.215	.264	0.071	6.8	0.018***	93.2	0.000	0.0
(26) Pro-deviant attitudes	4	5	0.240 (0.099)	−0.034; 0.514	.072	0.240	13.2	0.000	0.0	0.034	86.8
(27) Low romantic relationship quality	2	4	0.145 (0.059)	−0.042; 0.331	.090	0.144	18.5	0.011***	81.5	0.000	0.0
(28) Younger/older romantic partner	3	3	−0.052 (0.110)	−0.527; 0.423	.684	−0.052	3.0	0.018	48.5	0.018	48.5
(29) Lack of social support	2	3	0.084 (0.017)	0.011; 0.158	.039*	0.084	100.0	0.000	0.0	0.000	0.0
(30) Technological disinhibition	2	2	0.161 (0.043)	−0.380; 0.703	.164	0.160	100.0	0.000	0.0	0.000	0.0
(31) Non-intact family	2	3	0.102 (0.061)	−0.161; 0.366	.236	0.102	9.5	0.010**	90.5	0.000	0.0
(32) Deviant peers	4	7	0.309 (0.115)	0.027; 0.591	.036*	0.300	3.1	0.028**	44.6	0.033	52.4
(33) Attachment problems	7	20	0.147 (0.025)	0.095; 0.199	<.001***	0.146	10.1	0.009***	83.7	0.001	6.1
(34) Low parental monitoring	3	7	−0.013 (0.096)	−0.248; 0.221	.895	−0.013	3.4	0.013***	36.0	0.021	60.6
(35) Low SES	5	8	0.020 (0.014)	−0.013; 0.053	.192	0.020	100.0	0.000	0.0	0.000	0.0
(36) Digital dating abuse victim frequency	1	1	0.758 (0.068)	0.623; 0.891	<.001***	0.640	100.0				

(*continued on next page*)

Table 1 (*continued*)

Risk domains	# studies	# ES	Mean Fisher's Z (SE)	95 % CI	Sig. mean Z (*p*)	Mean *r*	% var. at level 1	Level 2 variance	% var. at level 2	Level 3 variance	% var. at level 3
(37) Digital dating abuse perpetration frequency	1	1	1.333 (0.069)	1.198; 1.468	<.001***	0.870	100.0				
(38) Lower level of goal efficacy	1	1	0.040 (0.027)	−0.013; 0.093	.139	0.040	100.0				
(39) Lower level of planning behavior	1	1	0.090 (0.027)	0.037; 0.143	<.001***	0.090	100.0				
(40) Not being an athlete	1	1	0.020 (0.037)	−0.052; 0.092	.589	0.020	100.0				
(41) No social skills	1	1	−0.060 (0.027)	−0.113; 0.000	.026*	−0.060	100.0				
(42) Low friendship quality	1	1	0.090 (0.142)	−0.188; 0.368	.634	0.090	100.0				

Note. #studies = number of studies, #ES = number of effect sizes in the study, SE = standard error, 95 % CI = 95 % confidence interval, Sig. = significance, *r* = effect size (Pearson's correlation), % var = percentage of variance.

* $p < .05$.

** $p < .01$.

*** $p < .001$.

male, $F(1, 16) = 5.562$, $p = .031$. The effect of being male is stronger in university students (mean $r = 0.209$) than in middle or high school students (mean $r = 0.051$) (see Table 4).

3.3. Hacking

For hacking, $N = 10$ studies were included that examined $k = 11$ independent samples. The studies were published between 2006 and 2018, and conducted in the United States ($k = 6$), South Korea ($k = 1$), China ($k = 1$), Canada ($k = 1$), Australia ($k = 1$), and one study was conducted in 31 different countries. A total of 536 effect sizes were extracted from these studies, with an average of 48.7 effect sizes per study. The total sample comprised $N = 72{,}218$ juveniles.

The overall association between all extracted risk factors and hacking perpetration was significant and very small in magnitude, $r = 0.073$, $p = .014$. Table 5 shows all created risk domains for hacking and their effects. Seven risk domains were significantly associated with hacking perpetration. A moderate effect was found for having deviant peers ($r = 0.335$), and small effects were found for prior online deviant behavior ($r = 0.299$), low moral standards ($r = 0.233$), low self-control ($r = 0.127$), and prior offline deviant behavior ($r = 0.119$). Finally, two very small effects were found for low school preoccupation ($r = -0.027$) and high computer preoccupation ($r = 0.062$).

Testing the significance of the within-study variance (level 2) and the between-study variance (level 3) revealed that in eleven risk domains significant level 2 and/or level 3 variance was present. However, moderator analyses were performed for only seven risk domains as these were based on at least five independent samples (see Table 6). The results indicated a moderating effect of educational stage in the domain being male, $F(1, 19) = 6.398$, $p = .020$. The effect of being male was stronger for middle or high school students (mean $r = 0.109$) than for university students (mean $r = -0.074$). This indicates that females are relatively more likely to perpetrate hacking in university than in middle and high school. There was also a moderating effect of educational stage on the effect of low self-control, $F(1, 82) = 13.793$, $p < .001$. The effect of low self-control was stronger for students in middle or high school (mean $r = 0.235$) than for university students (mean $r = 0.064$). Further, the percentage of males moderated the effect of computer preoccupation, $F(1, 87) = 9.401$, $p = .003$. The effect of a high computer preoccupation decreased as the percentage of males in samples increased ($\beta = -0.239$). Finally, both the percentage of males in samples, $F(1, 113) = 16.064$, $p < .001$, and the educational stage, $F(1, 113) = 6.139$, $p = .015$, moderated the effect of computer skills. As the percentage of males in samples increased, the effect of computer skills decreased ($\beta = -0.286$). Having computer skills was only a significant risk domain for juveniles in middle or high school (mean $r = 0.114$) and not for university students (mean $r = 0.002$).

4. Discussion

The present review is the first to provide a three-level meta-analytic overview of risk factors for juvenile perpetration of three different types of cybercrimes: cyberstalking, sexting, and hacking. The first aim of this study was to estimate the relations between risk factors in different risk domains and cyberstalking, sexting, and hacking perpetration by juveniles (aged 12–23 years). For each form of cybercrime, different risk domains have been studied, given the variables that were tested as risk factors in the available primary research: 35 risk domains for cyberstalking, 12 risk domains for sexting, and 21 risk domains for hacking. The second aim of this study was to examine whether the overall relations between the risk domains and the cybercrimes were moderated by gender, ethnicity, and educational stage.

4.1. Overall effect of risk domains

For cyberstalking, 15 significant risk domains were found. Overall, it appears that juveniles are at heightened risk of cyberstalking perpetration when they have committed prior online or offline crimes, or when they have been victims of online or offline crimes themselves. Also, when juveniles show attachment problems, have longer romantic relationships, and have more deviant peers, the risk of cyberstalking perpetration increases. Finally, other important risk factors are substance abuse, having mental health problems, having negative beliefs about the other gender, spending considerable time on computers or smartphones, and dark personality traits. Agnew's general strain theory could explain these findings as most of these factors heighten the risk of negative stimuli (such as parental rejection, negative experiences, negative peer relations, victimization), removal of positive stimuli (losing a romantic partner), or failure to achieve positively valued goals (such as status and respect, autonomy) which are theorized to cause strain and, in turn, pressure to engage in criminal coping (in this case: cyberstalking).

Regarding sexting, the other cyber-enabled criminal behavior, only two significant risk domains were found. Dark personality traits (small relation) and being male (very small relation) were risk factors for sexting perpetration. Further, a medium effect was found for the relation between peer pressure (individual factor) and sexting perpetration. However, this was only based on one study. Nevertheless, other studies also emphasized the role of peers in sexting perpetration. Lippman and Campbell (2014) found that young people can be encouraged to commit

Table 2
Results of moderator analyses in risk domains for cyberstalking.

Moderator variables	# studies	# ES	Intercept (95 % CI)/ mean *r* (95 % CI)	Mean *r*	β (95 % CI)	*F* (df1, df2)	*p*	Level 2 variance	Level 3 variance
(1) Being male									
Sample characteristics									
Percentage majority	8	9	0.001 (−0.039; 0.042)	–	0.239 (0.107;0.371)**	*F*(1, 8) = 17.402	.003**	0.001	0.000
Educational stage						*F*(1, 10) = 0.080	.783	0.004	0.007
Middle/high school	5	5	−0.021 (−0.130; 0.089)	−0.021					
University	6	7	−0.001 (−0.107; 0.104)	−0.001	0.019 (−0.133; 0.171)				
Type of cyberstalking						*F*(1, 10) = 16.022	.003**	0.001	0.002
Cyber dating abuse	7	8	−0.077 (−0.137; −0.016)*	−0.077					
Cyberstalking	4	4	0.095 (0.021; 0.168)*	0.095	0.171 (0.076; 0.267)**				
(3) Being Caucasian									
Sample characteristics									
Percentage males	6	13	−0.015 (−0.081; 0.051)	–	−0.128 (−0.739; 0.482)	*F*(1, 11) = 0.214	.652	0.010***	0.000
Percentage majority	6	13	0.009 (−0.080; 0.062)	–	0.052 (−0.162; 0.266)	*F*(1, 11) = 0.288	.602	0.010***	0.000
Educational stage						*F*(1, 11) = 0.010	.921	0.010***	0.001
Middle/high school	2	5	−0.016 (−0.133; 0.101)	−0.016					
University	4	8	−0.023 (−0.119; 0.073)	−0.023	−0.007 (−0.158; 0.145)				
Type of cyberstalking						*F*(1, 11) = 0.430	.526	0.010***	0.000
Cyber dating abuse	4	11	−0.007 (−0.079; 0.066)	−0.007					
Cyberstalking	2	2	−0.060 (−0.224; 0.104)	−0.060	−0.053 (−0.233; 0.126)				
(12) Dark personality traits									
Sample characteristics									
Percentage males	5	16	0.203 (0.042; 0.365)*	–	−0.059 (−0.550; 0.433)	*F*(1, 14) = 0.066	.802	0.002*	0.027***
(13) High computer preoccupation									
Sample characteristics									
Percentage males	6	16	0.159 (0.077; 0.241)***	–	−0.313 (−0.571; −0.055)*	*F*(1, 14) = 6.754	.021*	0.007***	0.004
Type of cyberstalking						*F*(1, 14) = 0.867	.368	0.008***	0.014*
Cyber dating abuse	4	13	0.104 (−0.035; 0.244)	0.104					
Cyberstalking	2	3	0.215 (0.001; 0.430)*	0.212	0.111 (−0.145; 0.367)				
(16) Previous cyberstalking victimization									
Sample characteristics									
Percentage males	6	10	0.610 (0.377; 0.843)***	–	0.076 (−0.936; 1.089)	*F*(1, 8) = 0.030	.866	0.099***	0.000
Percentage majority	5	8	0.694 (0.420; 0.968)***	–	722 (−0.687; 2.131)	*F*(1, 6) = 1.572	.256	0.089***	0.000
Educational stage									
Middle/high school	3	4	0.476 (0.140; 0.812)*	0.443					
University	3	6	0.703 (0.426; 0.980)***	0.606	0.227 (−0.209; 0.662)	*F*(1, 8) = 1.439	.265	0.084***	0.000
(17) Previous offline victimization									
Sample characteristics									
Percentage males	8	21	0.328 (0.177; 0.478)***	–	−0.035 (−0.594; 0.523)	*F*(1, 19) = 0.017	.896	0.018***	0.032*
Percentage majority	8	21	0.321 (0.174; 0.467)***	–	−0.128 (−0.691; 0.434)	*F*(1, 19) = 0.228	.639	0.018***	0.028*
Educational stage						*F*(1, 19) = 0.294	.594	0.018***	0.029*
Middle/high school	2	3	0.256 (−0.051; 0.563)	0.259					
University	6	18	0.347 (0.181; 0.513)***	0.334	0.090 (−0.259; 0.440)				
Type of cyberstalking						*F*(1, 19) = 3.375	.082	0.018***	0.015
Cyber dating abuse	6	12	0.381 (0.245; 0.517)***	0.364					
Cyberstalking	2	6	0.111 (0.045; 0.0176)**	0.111	−0.224 (−0.480; 0.031)				

(*continued on next page*)

Table 2 (*continued*)

Moderator variables	# studies	# ES	Intercept (95 % CI)/ mean *r* (95 % CI)	Mean *r*	β (95 % CI)	*F* (df1, df2)	*p*	Level 2 variance	Level 3 variance
(18) Previous offline violence perpetration									
Sample characteristics									
Percentage males	12	37	0.421 (0.253; 0.588)***	–	0.036 (−0.483; 0.555)	*F*(1, 35) = 0.019	.890	0.068***	0.055
Percentage majority	9	26	0.444 (0.204; 0.684)***	–	−0.117 (−0.940; 0.706)	*F*(1, 24) = 0.087	.771	0.094***	0.080
Educational stage						*F*(1, 35) = 0.207	.652	0.068***	0.052
Middle/high school	4	19	0.365 (0.069; 0.660)*	0.350					
University	8	26	0.445 (0.246; 0.643)***	0.418	0.080 (−0.276; 0.436)				
(20) Mental health problems									
Sample characteristics									
Percentage males	6	9	0.157 (0.062; 0.252)**	–	−0.075 (−0.382; 0.232)	*F*(1, 7) = 0.335	.581	0.004**	0.004
Percentage majority	6	9	0.172 (0.107; 0.236)***	–	0.190 (0.022; 0.359)*	*F*(1, 7) = 7.152	.032*	0.003**	0.000
Educational stage						*F*(1, 7) = 6.194	.042*	0.003**	0.000
Middle/high school	2	4	0.071 (−0.025; 0.168)	0.071					
University	4	5	0.205 (0.123; 0.287)***	0.202	0.133 (0.007; 0.260)*				
(22) Length of romantic relationship									
Sample characteristics									
Percentage males	8	9	0.135 (0.028; 0.241)*	–	0.066 (−0.217; 0.349)	*F*(1, 7) = 0307	.597	0.002	0.012
Percentage majority	7	8	0.116 (−0.043; 0.274)	–	0.265 (−0.672; 1.202)	*F*(1, 6) = 0.479	.515	0.002	0.014
Educational stage						*F*(1, 7) = 2.698	.144	0.002	0.007
Middle/high school	3	3	0.207 (0.068; 0.345)**	0.204					
University	5	6	0.079 (−0.041; 0.200)	0.079	−0.127 (−0.311; 0.056)				
(33) Attachment problems									
Sample characteristics									
Percentage males	7	20	0.149 (0.090; 0.207)***	–	−0.006 (−0.145; 0.134)	*F*(1, 18) = 0.008	.931	0.009***	0.002
Percentage majority	6	17	0.131 (0.079; 0.183)***	–	−0.097 (−0.349; 0.154)	*F*(1, 15) = 0.679	.423	0.007***	0.000
Educational stage						*F*(1, 18) = 0.200	.660	0.009***	0.001
Middle/high school	3	15	0.130 (0.026; 0.233)*	0.129					
University	4	5	0.156 (0.088; 0.223)***	0.155	0.026 (−0.097; 0.150)				
Type of cyberstalking						*F*(1, 18) = 2.503	.131	0.009***	0.000
Cyber dating abuse	5	10	0.181 (0.114; 0.248)***	0.179					
Cyberstalking	2	10	0.111 (0.045; 0.176)**	0.111	−0.071 (−0.164; 0.023)				

Note. # studies = number of studies, #ES = number of effect sizes, 95 % CI = 95 % confidence interval, *r* = effect size (Pearson's correlation), β = estimated regression coefficient, *F* = Omnibus *F* test, *p* = significance of omnibus *F* test.

* $p < .05$.

** $p < .01$.

*** $p < .001$.

sexting by their environment (Lippman & Campbell, 2014). Lenhart (2009) described that boys experience mutual pressure to ask for pictures of girls and to show or forward pictures of girls to each other. This pressure could be explained by the status they acquire among themselves through their sexual performances (Flood, 2007; Walker et al., 2013) and may be related to stereotypes and the norms in the peer group. Girls feel pressure from boys to create and share sexual material, partly out of fear of being rejected (Lippman & Campbell, 2014; Wolak & Finkelhor, 2011). We should note here, however, that the peer group norm could also have a positive effect, for example, it would have a protective effect if committing sexting was regarded as 'not done' from the prevailing group norm (Mitchell et al., 2015).

Concerning hacking, seven risk domains were significant. The results show that having deviant peers, low moral standards, a history of having committed online or offline crimes, and low self-control are risk factors for hacking. Additional effects were found for low school pre-occupation and high computer occupation, although very small. It is possible that youngsters low in self-control and with low moral standards associate with each other (selection) and influence each other in a negative way ('deviancy training'). These findings are in line with differential association theory and social learning theory. The findings are also in line with Gottfredson and Hirschi's general theory of crime that states that youngsters with low self-control are also insensitive and high on risk-taking and show all kinds of 'analogous' behaviors that satisfy short-term needs. Criminal behavior such as hacking becomes more likely when the propensity coincides with an opportunity, for instance, when juveniles are less occupied with their offline lives (at school) and more with their online lives (at their computers).

Interestingly, prior perpetration and victimization of online and offline crime show medium and strong relations with cyberstalking (and

Table 3
Results of the overall mean effect sizes of risk domains for sexting.

Risk domains	# studies	# ES	Mean Fisher's Z (SE)	95 % CI	Sig. mean Z (*p*)	Mean *r*	% var. at level 1	Level 2 variance	% var. at level 2	Level 3 variance	% var. at level 3
(1) Being male	16	19	0.071 (0.020)	0.028; 0.114	.003**	0.071	15.0	0.006*	85.0	0.000	0.0
(2) Being older	7	8	0.045 (0.030)	−0.027; 0.116	.186	0.045	16.8	0.000	0.00	0.005	83.2
(3) Being Caucasian	2	4	0.027 (0.012)	−0.011; 0.065	.108	0.027	100.0	0.000	0.00	0.000	0.00
(4) Dark personality traits	1	3	0.149 (0.032)	0.013; 0.285	.042*	0.148	66.6	0.001	33.4	0.000	0.0
(5) Low self-control	2	2	0.012 (0.022)	−0.265; 0.290	.673	0.012	100.0	0.000	0.0	0.000	0.0
(6) Being heterosexual	2	2	0.000 (0.013)	−0.160; 0.160	1.00	0.000	100.0	0.000	0.0	0.000	0.0
(7) Risk behavior	2	2	0.219 (0.137)	−1.522; 0.1.959	.356	0.216	2.7	0.018	48.6	0.018	48.6
(8) Sexual risk behavior	2	3	0.644 (0.482)	−1.431; 2.720	.274	0.568	0.3	0.002	0.4	0.463*	99.3
(9) Previous sexting victimization	4	4	0.327 (0.115)	−0.039; 0.692	.065	0.316	3.0	0.018	48.5	0.018	48.5
(10) High malevolent sexism	1	2	−0.015 (0.085)	−1.098; 1.068	.888	−0.015	9.7	0.013**	90.3	0.000	0.0
(11) Being single	1	2	0.077 (0.040)	−0.437; 0.590	.309	0.077	100.0	0.000	0.0	0.000	0.0
(12) Low SES	2	2	−0.038 (0.022)	−0.315; 0.240	.334	−0.038	100.0	0.000	0.0	0.000	0.0
(13) Male school	1	1	0.040 (0.027)	−0.013; 0.093	.139	0.040	100.0				
(14) Female school	1	1	−0.020 (0.027)	−0.073; 0.033	.459	−0.020	100.0				
(15) Criminological major	1	1	0.020 (0.052)	−0.082; 0.122	.701	0.020	100.0				
(16) Internet use	1	1	0.060 (0.052)	−0.041; 0.162	.250	0.060	100.0				
(17) Level of religiosity	1	1	0.029 (0.044)	−0.057; 0.115	.510	0.029	100.0				
(18) Positive attitudes on sexting	1	1	0.192 (0.027)	0.139; 0.245	<.001***	0.190	100.0				
(19) Peer pressure	1	1	0.536 (0.027)	0.483; 0.589	<.001***	0.490	100.0				
(20) Attachment problems	1	1	0.020 (0.027)	−0.032; 0.072	.459	0.020	100.0				

Note. #studies = number of studies, #ES = number of effect sizes in the study, SE = Standard Error, 95 % CI = 95 % confidence interval, Sig. = significance, *r* = effect size (Pearson's correlation), % var = percentage of variance.
* $p < .05$.
** $p < .01$.
*** $p < .001$.

Table 4
Results of moderator analyses in risk domains for sexting.

Moderator variables	# studies	# ES	Intercept (95 % CI)/mean Z (95 % CI)	Mean *r*	β (95 % CI)	*F* (df1, df2)	*p*	Level 2 variance	Level 3 variance
(1) Being male Educational stage						F(1, 16) = 5.562	.031*	0.004	0.001
Middle/high school	4	4	0.051 (0.007; 0.095)*	0.051					
University	3	17	0.212 (0.074; 0.349)**	0.209	0.161 (0.016; 0.305)*				

Note. # studies = number of studies, #ES = number of effect sizes, 95 % CI = 95 % confidence interval, *r* = effect size (Pearson's correlation), β = estimated regression coefficient, *F* = Omnibus *F* test, *p* = significance of omnibus *F* test.
* $p < .05$.
** $p < .01$.

small relations with hacking perpetration). Prior research has identified a 'bully-victim cycle', where persons who are a victim of bullying also become a bully themselves (Aleem, 2016). There is evidence that this is even more true for cyberbullying than for traditional bullying (e.g., Li, 2007; Mishna et al., 2012). This behavior can also be explained by social learning theory, where children copy the behavior of the bullies, become more aggressive and show more disruptive behavior themselves (Aleem, 2016; Akers, 1998). Additionally, a moderate impact of having deviant peers was found for both hacking and cyberstalking perpetration. Being affiliated with peers who are also involved in cybercriminal activities may lead to more acceptance of committing cybercrimes, even when the juvenile perpetrator knows the consequences for victims (Bossler &

Table 5
Results of the overall mean effect sizes of risk domains for hacking.

Risk domain	# studies	# ES	Mean Fisher's Z (SE)	95 % CI	Sig. mean Z (*p*)	Mean *r*	% var. at level 1	Level 2 variance	% var. at level 2	Level 3 variance	% var. at level 3
(1) Being male	7	21	0.023 (0.050)	−0.080; 0.127	.641	0.023	11.9	0.000	0.0	0.015***	88.1
(2) Being older	6	36	0.039 (0.032)	−0.027; 0.104	.241	0.039	28.9	0.000	0.8	0.005*	70.3
(3) Being Caucasian	1	3	−0.013 (0.032)	−0.150; 0.124	.716	−0.013	40.8	0.002	59.2	0.000	0.0
(4) Low self-control	6	84	0.128 (0.040)	0.048; 0.208	.002**	0.127	34.2	0.003**	20.4	0.006*	45.4
(5) Extraversion	3	3	−0.037 (0.107)	−0.499; 0.424	.761	−0.037	12.5	0.014	43.7	0.014	43.7
(6) Agreeableness	3	3	−0.400 (0.217)	−1.650; 0.849	.302	−0.380	1.6	0.123	49.2	0.123	49.2
(7) Neuroticism	3	3	0.007 (0.051)	−0.211; 0.226	.898	0.007	54.4	0.002	22.8	0.002	22.8
(8) Openness to experience	3	3	0.027 (0.035)	−0.123; 0.177	.520	0.027	98.9	0.000	0.5	0.000	0.5
(9) Conscientiousness	3	3	−0.046 (0.040)	−0.218; 0.127	.372	−0.046	80.8	0.000	9.6	0.000	9.6
(10) Being self-centered	2	16	−0.016 (0.024)	−0.067; 0.036	.524	−0.016	90.5	0.000	0.0	0.001	9.5
(11) Autistic traits	1	6	−0.059 (0.025)	−0.123, 0.006	.066	−0.059	67.8	0.001	32.2	0.000	0.0
(12) Prior online deviant behavior	5	19	0.308 (0.045)	0.213; 0.403	<.001***	0.299	5.1	0.024***	87.8	0.002	7.0
(13) Prior offline deviant behavior	2	13	0.120 (0.009)	0.100; 0.141	<.001***	0.119	1.5	0.001***	98.5	0.000	0.0
(14) Low school preoccupation	3	33	−0.027 (0.012)	−0.051; −0.003	.031*	−0.027	100.0	0.000	0.0	0.000	0.0
(15) High computer preoccupation	7	89	0.062 (0.022)	0.017; 0.106	.007**	0.062	38.7	0.002**	28.8	0.002***	32.6
(16) Low sports preoccupation	2	16	0.091 (0.086)	−0.092; 0.275	.306	0.091	26.3	0.000	0.0	0.014***	73.7
(17) Computer skills	5	115	0.045 (0.038)	−0.029; 0.119	.232	0.045	46.6	0.001	8.3	0.005***	45.1
(18) Low moral standards	5	25	0.237 (0.095)	0.041; 0.443	.020*	0.233	8.4	0.006***	12.1	0.042***	79.5
(19) Exploitive and manipulative behavior	2	2	0.150 (0.047)	−0.447; 0.748	.193	0.149	100.0	0.000	0.0	0.000	0.0
(20) High grades at school	3	17	0.017 (0.023)	−0.031, 0.065	.468	0.017	54.7	0.004*	45.3	0.000	0.0
(21) Deviant peers	2	7	0.348 (0.042)	0.246; 0.450	<.001***	0.335	17.3	0.010***	82.7	0.000	0.0
(22) Technological major	2	16	0.021 (0.018)	−0.017; 0.059	.265	0.021	100.0	0.000	0.0	0.000	0.0
(23) Criminological major	1	1	0.040 (0.052)	−0.062; 0.0142	.442	0.040	100.0				
(24) Non-intact family	1	1	0.000 (0.040)	−0.078; 0.078	1.00	0.000	100.0				
(25) Lower parental education	1	1	0.040 (0.052)	−0.062; 0.0142	.442	0.040	100.0				

Note. #studies = number of studies, #ES = number of effect sizes in the study, SE = Standard Error, 95 % CI = 95 % confidence interval, Sig. = significance, *r* = effect size (Pearson's correlation), % var = percentage of variance.
* $p < .05$.
** $p < .01$.
*** $p < .001$.

Burruss, 2012; Gordon, 2000; Holt et al., 2010).

Several non-significant risk domains are interesting as well. Being male was only a significant risk factor for sexting perpetration, whereas in the literature males are generally considered as perpetrators of cybercrimes and females as victims (Hutchings & Chua, 2016). Further, we expected that low self-control would be an important risk factor for cybercriminal behavior, but this was only found for hacking (cyber-dependent crimes) and not for cyberstalking or sexting (both cyber-enabled crimes). A possible explanation is that hacking is a thrill-seeking offense, whereas cyberstalking and sexting are more relational offenses. In prior research it has been found that thrill-seeking is an important moderator of the relation between self-control and crime. Juveniles who are low in self-control and show thrill-seeking behavior are more likely to commit a crime than juveniles with low self-control and little thrill-seeking behavior (Burt & Simons, 2013). Lastly, it is often presumed that hackers have limited social skills, but strong computer skills (Barber, 2001). This assumption was not evidenced by the present findings, since no significant relations with hacking perpetration were found for autistic traits, computer skills, and personality traits (such as self-centeredness, introversion, and agreeableness). However, this may be explained by the possibility that the studies included in this review mainly captured the so-called 'scriptkiddies', who are teenagers with limited computer knowledge trying – and often succeeding – in hacking by using online tutorials (Barber, 2001). By all means, more research is necessary, as only a few studies on juvenile hacking looked at autistic and personality traits.

Table 6
Results of moderator analyses in risk domains for hacking.

Moderator variables	# studies	# ES	Intercept (95 % CI)/mean Z (95 % CI)	Mean *r*	β (95 % CI)	*F* (df1, df2)	*p*	Level 2 variance	Level 3 variance
(1) Being male									
Educational stage						*F*(1, 19) = 6.398	.020*	0.000	0.007
Middle/high school	3	3	0.109 (0.003; 0.214)*	0.109					
University	4	18	−0.074 (−0.182; 0.034)	−0.074	−1.82 (−0.333, −0.031)*				
(2) Being older									
Sample characteristics									
Percentage males	6	36	0.010 (−0.077; 0.097)	–	−0.205 (−0.611; 0.201)	*F*(1, 34) = 1.056	.311	0.000	0.005**
Educational stage						*F*(1, 34) = 0.089	.767	0.000	0.007
Middle/high school	3	3	0.050 (−0.056; 0.156)	0.050					
University	3	33	0.028 (−0.074; 0.131)	0.028	−0.022 (−0.169; 0.126)				
(4) Low self-control									
Sample characteristics									
Percentage males	5	84	0.105 (0.010; 0.200)*	–	−0.218 (−0.689; 0.254)	*F*(1, 82) = 0.843	.361	0.003**	0.007**
Educational stage						*F*(1, 82) = 13.793	<.001***	0.003**	0.000
Middle/high school	3	3	0.240 (0.149; 0.330)***	0.235					
University	3	81	0.064 (0.039; 0.089)***	0.064	−0.176 (−0.270; −0.082)***				
(12) Prior online deviant behavior									
Sample characteristics									
Percentage males	5	19	−0.447 (−4.187; 3.292)	–	−3.715 (−22.144; 14.714)	*F*(1, 17) = 0.181	.676	0.026***	0.003
(15) High computer preoccupation									
Sample characteristics									
Percentage males	7	89	0.039 (0.016; 0.063)**	–	−0.239 (−0.394; −0.084)**	*F*(1, 87) = 9.401	.003**	0.002*	0.000**
Educational stage						*F*(1, 87) = 3.710	.057	0.002**	0.001**
Middle/high school	4	8	0.101 (0.044; 0.158)***	0.101					
University	3	81	0.029 (−0.018; 0.077)	0.029	−0.072 (−0.146; 0.002)				
(17) Computer skills									
Sample characteristics									
Percentage males	5	115	0.017 (0.002; 0.032)*	–	−0.286 (−0.427; −0.144)***	*F*(1, 113) = 16.064	<.001***	0.001	0.000
Educational stage						*F*(1, 113) = 6.139	.015*	0.001	0.001**
Middle/high school	3	8	0.115 (0.036; 0.194)**	0.114					
University	2	10	0.002 (−0.041, 0.046)	0.002	−0.113 (−0.203; −0.023)*				
(18) Low moral standards									
Sample characteristics									
Percentage males	5	25	0.262 (0.073; 0.452)**	–	0.643 (−0.484, 1.769)	*F*(1, 23) = 1.392	.250	0.006***	0.037***

Note. # studies = number of studies, #ES = number of effect sizes, 95 % CI = 95 % confidence interval, *r* = effect size (Pearson's correlation), β = estimated regression coefficient, *F* = Omnibus *F* test, *p* = significance of omnibus *F* test.
* $p < .05$.
** $p < .01$.
*** $p < .001$.

When comparing the currently identified risk factors for the different forms of cybercrime with the risk factors for offline crimes, there are some noteworthy findings. First, there seems to be some overlap in risk factors, as prior involvement in crimes, dark personality traits, deviant norms and beliefs, and having deviant peers are risk factors for both cybercrime and offline crime. On the other hand, differences in risk factors have also been found, as personality traits (Big Five) and self-control could not be identified as risk factors for all studied cybercrimes. However, it should be noted here that the majority of primary research has tested the more 'traditional' risk factors for cybercrime and little other or new – possibly cybercrime specific – risk factors (such as online disinhibition). If so, it is possible that even more differences will be found in the explanation of cyber and the 'traditional' crimes. Also, to really test for differences in the explanatory value of different risk factors, studies on 'traditional' crimes should be included besides studies on cybercrimes.

It is also interesting to look at the overlap in risk factors across the different types of cybercrime to determine whether the same risk factors are associated with different types of cybercrimes, or whether each cybercrime type has unique risk factors. As discussed above, some risk factors seem to pose a risk for crime in general, such as prior deviant (online and offline) behavior, having deviant peers, low moral standards, and dark personality traits. Only one risk factor was identified that seems to be specific for cybercrime, which is a high computer

preoccupation. The results for low self-control and being male are inconclusive, meaning that these variables pose risk factors for some cybercrime types, but not for other cybercrime types. It is also noteworthy that the included studies did not examine the same variables as risk factors for cyberstalking, sexting, and hacking, which makes it more difficult to make statements about the overlap between the different cybercrimes. Therefore, more research is needed to examine overlap in risk factors across different types of cybercrimes. As such, the current study should be considered as a first step in exploring this new meta-analytic field.

4.2. Moderator effects

For risk domains with sufficient data, moderator analyses were performed. A first interesting finding in this respect is that educational stage was found to be the most common significant moderator. Considering hacking, three risk domains were moderated by educational stage. For being male, having low self-control, and having good computer skills, it was found that being in middle and high school constitutes a greater risk for hacking perpetration. A smaller impact of these risk domains was found in university students. It seems that low self-control is especially associated with delinquent behavior in high school and in boys (Feldman & Weinberger, 1994). The risk factor being male was also moderated by educational stage for sexting. Males committed significantly more sexting offenses in university than in middle/high school. Finally, the relation between high computer preoccupation and both cyberstalking and hacking perpetration was moderated by the percentage of males in the sample: when the percentage of males in the sample increased, the relation between high computer preoccupation and cyberstalking and hacking decreased. This result indicates that high computer preoccupation is in particular a risk factor for hacking perpetration by girls. This finding can be explained by referring to the gender paradox (Hoeve et al., 2012), which assumes that girls in general commit less crimes or show less behavioral problems. However, if girls do commit crimes or show behavioral problems, these are often more severe than with the males. It is possible that the girls who hack are the girls with more extreme problems, also indicated by a high computer preoccupation.

4.3. Limitations

This study has several limitations. First, several risk domains did not consist of many effect sizes and moderator analyses were sometimes based on a low number of studies and effect sizes. Also, because some risk domains were rather small, it was not possible to review publication bias for each risk domain in a reliable manner or resolve publication bias with a trim-and-fill analysis (Duval & Tweedie, 2000b). The field of juvenile cybercrime is relatively new, and therefore relatively little primary research on risk factors for juvenile cybercrime perpetration was available. This study should therefore be seen as a first exploratory overview of risk factors for three types of cybercrime committed by juveniles. There have not been prior reviews or meta-analyses on risk factors for juvenile cybercrimes, although a review on risk factors for cyberbullying is available (Chen et al., 2017). It is therefore recommended that this review is updated when the body of primary research has increased to see whether current results can be replicated and/or should be adjusted. It may be very well possible that 'new' risk factors for cybercrime can be identified in future research. Until now, mainly traditional risk factors have been studied. Further, the quality of the available primary studies was sometimes rather low, for example, because a clear description of the instruments used for measuring cybercrime perpetration was lacking.

Second, it should be stressed that the reported relations are correlational and not causal. It is therefore not possible to interpret the identified risk factors as predictors for cyberdelinquent behavior. Instead, the studied factors are correlates of cyberdelinquent behavior. Nevertheless, these factors could be important in prevention and intervention efforts, and future longitudinal research may confirm these correlates as true predictors of cybercrime.

4.4. Implications

The results of this review have implications for clinical practice. The results could especially contribute to strengthening prevention and intervention programs that are aimed at reducing (the risk of) cybercriminal behavior. First, it seems important to monitor juveniles who previously have been a perpetrator or victim of online or offline crimes and to be aware that offline youth delinquents may also (start to) commit online offenses. In a review of studies on traditional crimes it was found that the majority of the studies supported the victim-offender overlap (Jennings et al., 2012). Studies looking into the victim-offender overlap for traditional juvenile crime found small to medium correlations (Barnes & Beaver, 2012; Beckley et al., 2017; Posick, 2013). Since the present review found medium and large effects for prior online victimization and perpetration, it seems that the victim-offender overlap for online crime is at least as large, and possibly even larger, as for traditional crime. Further, juveniles committing cybercrime seem to be highly influenced by their (deviant) peers. Juveniles might be less likely to imitate the behavior of deviant peers when the reward for committing cybercrime is reduced (Clarke, 1997). Another aspect that might be important for prevention programs is to reduce the time spent online, since high computer preoccupation was found to be a risk factor.

Oosterwijk and Fischer (2017) wrote a review of interventions for juvenile cybercrime perpetrators, including interventions for cyber aggression, sexting, and hacking. Regarding cyberstalking, interventions seemed to focus mainly on female victims and male perpetrators (Halder, 2015; King, 2008), whereas no gender effect was found for juvenile perpetrators in the current study. Interventions should therefore not only focus on male, but also on female perpetrators.

Regarding sexting, the available interventions solely focused on victims and prevention programs only focused on stopping the sending of sexts (Döring, 2014; Oosterwijk & Fischer, 2017). Until now, no intervention had taken the role of perpetrators into account who forced a person to make sexts or distribute sexts of other persons (Oosterwijk & Fischer, 2017). In the Netherlands, a new intervention specifically for sexting among 12–17 year olds was developed, called 'respect online' (Jonker & van Diessen, 2017). The aims of this intervention are to teach rules for safe and respectful online behavior, recognizing peer pressure, and offer support for parents. The current study showed evidence for the importance of peer pressure. Still, relatively little is known about the perpetrators of sexting. Therefore, more research is necessary to better inform and evaluate sexting prevention and intervention programs.

Most interventions have been designed for hacking perpetrators (Oosterwijk & Fischer, 2017). Some interventions focus on warning juveniles when they are about to commit a hacking offense and on the distinction between 'good' and 'bad' cyber-behavior, whereas others focus on teaching societal values. The present study found that in particular juveniles with deviant peers, low self-control and low moral standards are involved in hacking. It might be that they have other moral beliefs in 'hacking ethics' than in 'societal ethics'. They are often punished legally and still think they did nothing wrong (Kao et al., 2009). Juveniles may need to learn the differences between right and wrong behavior in the context of hacking. Changing deviant group norms and the ethical code of a hacker might have great potential in preventing recidivism of cybercriminal behavior. An intervention that was recently developed in the Netherlands, Hack_Right, applies exactly this strategy of changing the ethical code of a hacker (Halt, 2018). This seems a promising approach, but a proper evaluation of this intervention is necessary to determine its effectiveness.

5. Conclusion

The present study identified risk factors for three forms of cybercriminal behaviors: cyberstalking, sexting, and hacking. Overall, peer factors were found to be important for all three types of cybercrimes (deviant peers for cyberstalking and hacking and peer pressure for sexting). Besides, for cyberstalking, previous online and offline perpetration and victimization were significant risk factors. Other small but significant effects for multiple cybercrime types were found for dark personality traits (for cyberstalking and sexting) and high computer preoccupation (for cyberstalking and hacking). Additionally, the results showed that the impact of several risk domains is moderated by educational stage: some risk domains are more important for juveniles attending middle or high school than for juveniles attending university. This review presents a first overview of risk factors for cybercrime. However, it needs to be said that for a reevaluation of our findings, we wish for more primary studies on specific types of juveniles cybercrimes.

Declaration of competing interest

None.

Data availability

Data will be made available on request.

Acknowledgements

We thank Drs. Janneke P. C. Staaks for her help with the literature search.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.avb.2023.101836.

References[1]

Akers, R. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston, MA: Northeastern University Press.

Aleem, S. (2016). Bullying behaviour among school students: A review. *Indian Journal of Health & Wellbeing, 7*(10), 976–981. Retrieved from https://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=1&sid=4ff4ba81-04e8-453d-bc8f-0fd80c3eff40%40sessionmgr4007. Retrieved from.

Andrews, D., & Bonta, J. (Eds.). (2010). *The psychology of criminal conduct* (5th ed.). New Providence, NJ: Matthew Bender & Company, Inc, LexisNexis Group.

Assink, M., & Wibbelink, C. J. M. (2016). Fitting three-level meta-analytic models in R: A step-by-step tutorial. *The Quantitative Methods for Psychology, 12*(3), 154–174. https://doi.org/10.20982/tqmp.12.3

Barber, R. (2001). Hackers profiled – Who are they and what are their motivations? *Computer Fraud & Security, 2*, 14–17. https://doi.org/10.1016/S1361-3723(01)02017-6

Barnes, J. C., & Beaver, K. M. (2012). Extending research on the victim-offender overlap: Evidence from a genetically informative analysis. *Journal of Interpersonal Violence, 27*(16), 3299–3321. https://doi.org/10.1177/0886260512441259

Bates, S. (2017). Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology, 12*(1), 22–42. https://doi.org/10.1177/1557085116654565

Beckley, A. L., Caspi, A., Arsenault, L., Barnes, J. C., Fisher, H. L., Harrington, H., … Moffitt, T. E. (2017). The developmental nature of the victim-offender overlap. *Journal of Developmental and Life-Course Criminology, 4*(3), 24–49. https://doi.org/10.1007/s40865-017-0068-3

Bocij, P., & McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal, 139*, 31–38.

Boman, J. H., & Freng, A. (2017). Differential association theory, social learning theory, and technocrime. In *Technocrime and criminological theory* (pp. 55–65). Routledge.

Bossler, M. A., & Burruss, G. W. (2012). The general theory of crime and computer hacking: Low self-control hacking?. In *Cyber crime: Concepts, methodologies, tools and applications* (pp. 1499–1527). Hershey, PA: IGI Global.

Burt, C. H., & Simons, R. L. (2013). Self-control, thrill seeking, and crime: Motivation matters. *Criminal Justice and Behavior, 40*(11), 1326–1348. https://doi.org/10.1177/0093854813485575

Chen, L., Ho, S. S., & Lwin, M. O. (2017). A meta-analysis of factors predicting cyberbullying perpetration and victimization: From the social cognitive and media effects approach. *New Media & Society, 19*(8), 1194–1213. https://doi.org/10.1177/1461444816634037

Clarke, R. V. (1997). *Situational crime prevention. Successful case studies* (2nd ed.). Guilderland, NY: Harrow and Heston.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Hillsdale, NJ: Lawrence Erlbaum.

Digman, J. M. (1990). Personality structure: Emergence of the five-factor model. *Annual Review of Psychology, 41*(1), 417–440. https://doi.org/10.1146/annurev.ps.41.020190. 002221

Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8*(1). https://doi.org/10.5817/CP2014-1-9

Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberspsychology, Behavior, and Social Networking, 17*(2), 61–67. https://doi.org/10.1089/cyber.2012.0231

Duval, S., & Tweedie, R. (2000a). Trim and fill: A simple funnel plot based method of testing and adjusting for publication bias in meta-analysis. *Biometrics, 56*, 455–463. Retrieved from http://www.biometrics.tibs.org.

Duval, S., & Tweedie, R. (2000b). A nonparametric 'trim and fill' method of accounting for publication bias in meta-analysis. *Journal of the American Statistical Association, 95*, 89–98. https://doi.org/10.1080/01621459.2000.10473905

Feldman, S. S., & Weinberger, D. A. (1994). Self-restraint as a mediator of family influences on boys' delinquent behavior: A longitudinal study. *Child Development, 65*, 195–211. https://doi.org/10.1111/j.1467-8624.1994.tb00744.x

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19*, 468–483. https://doi.org/10.1177/0886260503262083

Flood, M. (2007). Men, sex, and homosociality: How bonds between men shape their sexual relations with women. *Men and Masculinities, 10*(3), 339–359. https://doi.org/10.1177/1097184 X0628776

Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium. *Computers & Security, 18*, 28–34. https://doi.org/10.1016/S0167-4048998006-6

Gordon, S. (2000, September). Virus writers: The end of the innocence? Paper presented at the 10th Annual Virus Bulletin Conference, Orlando, FL. Retrieved from https://pdfs.semanticscholar.org/c0f9/db4fdb5945eace504eff659b5ed7ddf43e37.pdf.

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

Halder, D. (2015). Cyber stalking victimisation of women: Evaluating the effectiveness of current laws in India from restorative justice and therapeutic jurisprudential perspectives. *Temida*, 103–130. https://doi.org/10.2298/TEM1504103H

Halt. (2018, December 18). Hack_Right: jonge hackers weer op het rechte pad. Retrieved from https://www.halt.nl/actueel/hack_right-jonge-hackers-weer-op-het-rechte-pad/.

Hoeve, M., Vogelvang, L., Wong, T., & Kruithof, B. (2012). Het mysterie van de criminele vrouw: Theorieën over criminaliteit door meisjes en vrouwen [The mystery of the criminal woman: Theories about criminality by girls and women]. In A.-M. Slotboom, M. Hoeve, M. Ezinga, & P. van der Helm (Eds.), *Criminele meisjes en vrouwen: achtergronden en aanpak [Criminal girls and women: Backgrounds and approach]* (pp. 69–94). Boom Lemma.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice, 33*, 31–61. https://doi.org/10.1080/0735648X.2010.9721287

Hutchings, A., & Chua, Y. T. (2016). Gendering cybercrime. In T. J. Holt (Ed.), *Cybercrime through an interdisciplinary lens* (pp. 167–188). Oxon: Routledge.

Jennings, W. G., Piquero, A. R., & Reingle, J. M. (2012). On the overlap between victimization and offending: A review of the literature. *Aggression and Violent Behavior, 17*, 16–26. https://doi.org/10.1016/j.avb.2011.09.003

Johnson, J. *Daily internet usage per capita worldwide 2011-2021, by device*. (2021). Statista. https://www.statista.com/statistics/319732/daily-time-spent-online-device/.

Jonker, M., & van Diessen, C. (2017). Toeleidingshandleiding halt-interventie sexting: Respect online: Een interventie voor jongeren die lichte vormen van seksueel grensoverschrijdend gedrag hebben vertoond. Retrieved from https://www.rutgers.nl/sites/rutgersnl/files/PDF/Halt-interventie%20sexting%20Toeleidingshandleiding.pdf.

Kao, D. Y., Fu-Yuan Hang, F., & Wang, S. J. (2009). Persistence and desistance: Examining the impact of re-integrative shaming to ethics in Taiwan juvenile hackers. *Computer Law and Security Review, 25*, 464–476. https://doi.org/10.1016/j.clsr.2009.05.009

King, M. S. (2008). Restorative justice, therapeutic jurisprudence and the rise of emotionally intelligent justice. *Melbourne University Law Review, 32*, 1096–1126. Retrieved from http://www.mulr.com.au/issues/32_3/32_3_10.pdf. Retrieved from.

[1] References marked with an asterisk indicate studies included in the meta-analysis.

Kuss, D. J., & Griffiths, M. D. (2012). Internet gaming addiction: A systematic review of empirical research. *International Journal of Mental Health and Addiction, 10*, 278–296. https://doi.org/10.1007/s11469-011-9318-5

*Lee, B. H. (2018). Explaining cyber deviance among school-aged youth. *Child Indicators Research, 11*, 563–584. https://doi.org/10.1007/s12187-017-9450-2

Lenhard, W., & Lenhard, A. (2016). *Calculation of effect sizes*. Dettelbach, Germany: Psychometrica. https://doi.org/10.13140/RG.2.1.3478.4245

Lenhart, A. (2009). *Teens and sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging*. Washington, DC: Pew Research Center.

Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior, 23*, 1777–1791. https://doi.org/10.1016/j.chb.2005.10.005

Lippman, J. R., & Campbell, S. W. (2014). Damned if you do, damned if you don't … if you're a girl: Relational and normative contexts of adolescent sexting in the United States. *Journal of Children and Media, 8*(4), 371–386.

Lipsey, M. W., & Wilson, D. B. (2001). *Practical meta-analysis*. Thousand Oaks, CA: SAGE publications.

Macaskill, P., Walter, S. D., & Irwig, L. (2001). A comparison of methods to detect publication bias in meta-analysis. *Statistics in Medicine, 20*, 641–654.

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy. Retrieved from. Pew Internet & American Life Project. www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.

McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies, 37*, 534–561. https://doi.org/10.1093/ojls/gqw033

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence (Research Report 75). Chapter 1: cyber-dependent crimes. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf.

Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2012). Risk factors for involvement in cyber bullying: Victims, bullies and bully-victims. *Children and Youth Services Review, 34*, 63–70. https://doi.org/10.1016/j.childyouth.2011.08.032

Mitchell, V., Petrovici, D., Schlegelmilch, B. B., & Szőcs, I. (2015). The influence of parents versus peers on generation Y internet ethical attitudes. *Electronic Commerce Research and Applications, 14*, 95–103. https://doi.org/10.1016/j.elerap.2014.12.003

Moffitt, T. E. (1993). Adolescence-limited and life-course persistent antisocial behavior: A developmental taxonomy. *Psychological Review, 100*, 674–701.

Navarro, J. N., & Marcum, C. D. (2020). Deviant instruction: The applicability of social learning theory to understanding cybercrime. In *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 527–545). Cham: Palgrave Macmillan.

Nodeland, B., & Morris, R. (2020). A test of social learning theory and self-control on cyber offending. *Deviant Behavior, 41*, 41–56.

Oosterwijk, K., & Fischer, T. F. C. (2017). *Interventies Jeugdige Daders Cybercrime*. Den Haag, The Netherlands: WODC.

Paulhus, D. L. (2014). Toward a taxonomy of dark personalities. *Current Directions in Psychological Science, 23*, 421–426. https://doi.org/10.1177/0963721414547737

Posick, C. (2013). The overlap between offending and victimization among adolescents: Results from the second international self-report delinquency study. *Journal of Contemporary Criminal Justice, 29*, 106–124. https://doi.org/10.1177/1043986212471250

*Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behavior, 33*, 1–25. https://doi.org/10.1080/01639625.2010.0538364

*Rogers, M., Seigfried, K., & Tidke, K. (2006). Self-reported computer criminal behaviour: A psychological analysis. *Digital Investigation, 3*, 116–120. https://doi.org/10.1016/j.diin.2006.06.002

*Rogers, M., Smoak, N. D., & Liu, J. (2006). Self-reported deviant computer behaviour: A big-5, moral choice, and manipulative exploitive behaviour analysis. *Deviant Behavior, 27*, 245–268. https://doi.org/10.1080/01639620600605333

Rosenthal, R. (1979). The file drawer problem and tolerance for null results. *Psychological Bulletin, 86*, 638–641. https://doi.org/10.1037/0033-2909.86.3.638

Seigfried, K. C., Lovely, R. W., & Rogers, M. K. (2008). Self-reported online child pornography behaviour: A psychological analysis. *International Journal of Cyber Criminology, 2*, 286–297. Retrieved from https://www.cybercrimejournal.com. Retrieved from.

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law, 13*, 627–640. https://doi.org/10.1080/10683160701340528

Silver, N. C., & Dunlap, W. P. (1987). Averaging correlation coefficients: Should Fisher's z transformation be used? *Journal of Applied Psychology, 72*, 146–148. https://doi.org/10.1037/0021-9010.72.1.146

Sutherland, E. H. (1947). Differential association theory. In F. P. Williams, III, & M. D. McShane (Eds.), *Criminology theory: Selected classic readings*. Routledge.

Tabachnik, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). Boston, MA: Allynand Bacon.

Van den Noortgate, W., López-López, J. A., Marín-Martínez, F., & Sánchez-Meca, J. (2013). Three-level meta-analysis of dependent effect sizes. *Behavior Research Methods, 45*, 576–594. https://doi.org/10.3758/s13428-012-0261-6

Viechtbauer, W. (2010). Conducting meta-analyses in R with the metafor package. *Journal of Statistical Software, 36*, 1–48. http://www.jstatsoft.org/v36/i03/.

Walker, S., Sanci, L., & Temple-Smith, M. (2013). Sexting: Young women's and men's views on its nature and origins. *Journal of Adolescent Health, 52*(6), 697–701. https://doi.org/10.1016/j.jadohealth.2013.01.026

Walkers, D. A. (2003). JMASM9: Converting Kendall's tau for correlational or meta-analytic analyses. *Journal of Modern Applied Statistical Methods, 2*, 525–530. https://doi.org/10.22237/jmasm/1067646360

Wall, D. S. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. *The European Review of Organised Crime, 2*, 71–90. https://doi.org/10.2139/ssrn.2677113

Wolak, J., & Finkelhor, D. (2011). Sexting: A typology. Retrieved from: https://scholars.unh.edu/cgi/viewcontent.cgi?article=1047&context=ccrc.

Zezulka, L. A., & Seigfried-Spellar, K. C. (2016). Differentiating cyberbullies and internet trolls by personality characteristics and self-esteem. *Journal of Digital Forensics, Security, and Law, 11*, 7–25.