CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

Identifying risk factors associated with adolescent cyber-deviance in Australia

Implications for Policy and Practice

Russell Brewer, Tyson Whitten, Morgan Sayer, Colette Langos

Digital Youth Research Laboratory, University of Adelaide

Contact
rachael.falk@cybersecuritycrc.org.au
02 6103 9922

Edith Cowan University
270 Joondlaup Drive,
Joondalup WA 6027
PO BOX 4155, Kingston ACT 2604

cybersecuritycrc.org.au

EXECUTIVE SUMMARY

Background

Little systematic attention has been given to the specific digital settings and contexts in which cyber-deviance occurs. As a result, many of the preventative programs developed or recommendations made are not necessarily evidence based. Identifying and articulating evidence-based approaches to developing effective interventions for young people is critical due to the serious social and economic harms associated with increasing levels of cyber-deviance (Brewer et al. 2018; Cale et al. 2019; Livingstone et al. 2010; 2011). Importantly, much research suggests the development of effective interventions relies on the accurate identification of factors known to contribute to delinquency (Andrews & Bonta 2010; Dowden & Andrews 1999; Koehler et al. 2013). A substantial body of research has identified risk factors associated with deviance in offline settings. Dynamic risk factors that are relatively stable across time (including those relating to behavioural functioning, propensity for risk-taking and parenting practices) tend to have a strong influence on the risk of delinquency in offline settings, and may also be a precursor for serious and persistent anti-social behaviours (Farrington, 2010; Moffitt et al. 1996). Fortunately, given that these stable risk factors often first manifest at an early age, vulnerable youth can be prospectively identified early in life, and subsequently prioritised for indicated prevention programs.

When it comes to cyber-deviance, however, the evidence base regarding its prevention is far less developed, particularly as it pertains to young people. In addition to not knowing the impact of such risk factors on cyber-deviance, in recent years, researchers have hypothesised that there may be distinctive and divergent criminogenic factors at play whilst online, when compared to offline forms of deviance. This work argued that features of online environments can have profound implications for how adolescent delinquency arises and can therefore make the digital environment a hazardous place from a risk management and mitigation perspective (Goldsmith & Brewer, 2015). Recent studies have begun to account for these criminogenic properties and understand cyber-deviance as driven not only by individual (i.e. dynamic) attributes, but also as a function of *exposure* to digital technologies, sites and services, and the interactional opportunities afforded as a consequence (e.g. Brewer et al. 2018; Cale et al. 2019). This body of work suggests that in order to fully understand the risk factors online, both idiosyncratic and exposure measures must be accounted for.

This report aims to identify whether time-stable dynamic risk factors are associated with adolescent cyber deviance in Australia, as well as better understand the risks associated with exposure across digital environments. This research was conducted for the purposes of developing an evidence base from which researchers can draw upon to design more effective interventions. This was achieved by conducting a cross-sectional study in a South Australian secondary school (n=327) that assessed the factors associated with adolescent engagement in eight forms of cyber-deviance: cyber-hate, cyber-violence, digital piracy, unauthorised access (hacking), cyber-bullying and abuse, online fraud, sexting, and image-based sexual abuse.

Key Findings

When considered together, these results depict several important trends relating to adolescent engagement in cyber-deviance.

Behavioural Functioning risk factors - all of the risk factors pertaining to behavioural functioning affected cyber-deviance across nearly all forms.

- Problems linked to *hyperactivity and inattention* were the most pervasive and were found to be associated with an increased likelihood of participants engaging in digital piracy, cyber-bullying, online fraud, sexting, as well as passive and active forms of cyber-violence.
- *Conduct problems* were also widespread and were found to be associated with an increased likelihood of engagement in hacking, cyber-bullying, online fraud, sexting and active participation in cyber-hate.
- *Emotional problems* were associated with an increased likelihood of adolescent engagement in cyber-bullying and sexting, as well as passive forms of cyber-hate and cyber-violence.
- Having *peer problems* was associated with an increased likelihood of engaging in cyber-bullying and online fraud.
- Exhibiting more *prosocial behaviours* was associated with an increased likelihood of engagement in digital piracy and sexting.
- An adolescent's increased propensity for *risk-taking* proved to be associated with engagement in all forms of cyber-deviance, except for active participation in cyber-hate.

Parenting practice risk factors - several of these factors were found to be associated with an increased likelihood of adolescent engagement in some forms of cyber-deviance.

- Higher levels of *parental autonomy* (i.e. adolescents being endowed with greater autonomy) was associated with an increased likelihood of adolescent engagement in sexting, but a decrease in cyber-bullying and online fraud.
- Higher levels of *parental discipline* (i.e. parent favouring strict disciplinary attitudes) are associated with an increased likelihood of engagement in hacking and passive forms of cyber-hate.
- The degree of parental supervision experienced by participants (i.e. the extent to which their activities are monitored by parents) had no observed association with any form of cyber-deviance.

Exposure risk factors - The types of experiences that young people had whilst online (i.e. online exposure) were also found to be associated with an increased likelihood of engagement in various forms of cyber-deviance.

- Increased frequency of *routine exposure* was associated with an increased likelihood of engagement in hacking, piracy, and passive participation in cyber-have and cyber-violence.
- Increased *social exposure* was also associated with an increased likelihood with engagement in a different configuration of cyber-deviance types. This overlapped with engagement with routine exposure, which was also associated with hacking, and passive engagement with cyber-hate and cyber violence. It was also associated with cyber-bullying and sexting.
- Increased s*pecialised exposure* was also associated with an increased likelihood of engagement in overlapping forms of cyber-deviance, including hacking, piracy, cyber-bullying and sexting, as well as being the sole situational factor found to be associated with an increased likelihood of engagement in online fraud.

Implications for policy and practice

The identification of time stable, dynamic risk factors for engagement in cyber-deviance has significant implications for the future design of interventions. While the key to effective intervention design is to target risk factors that have been empirically shown to increase the propensity for problematic behaviour, it is prudent to keep in mind that targeting risk factors that commonly occur across different forms of cyber-deviance could be a resource-efficient way to reduce multiple types of problematic behaviour. It is not the intention of this paper to design interventions for implementation, but several suggestions have been made for the direction future research may take.

Specifically, given the significant effect parenting practices were found to have on cyber-deviance, future research may consider how parents can be effectively included in intervention programs. Additionally, propensity for risk-taking, emotional, peer and conduct problems were significant risk factors in multiple forms of cyber-deviance. Social and emotional learning (SEL) programs have been used in previous developmental research to improve self-control, social and emotional skills as well as decreasing conduct problems in adolescents (Coelho and Sousa 2017; Durlak et al. 2011). The incorporation of SEL elements into intervention design has the potential to address several risk factors. Finally, measures of online exposure were significantly associated with an increased propensity for cyber-deviance. Situational crime prevention (SCP) is an approach that has been successfully employed to address offline offences, but has, as yet, received limited attention in the context of cyber-deviance. SCP techniques have the potential to reduce criminogenic opportunities, thereby reducing the likelihood of cyber-deviance.

While this paper presents a number of potentially useful directions for cyber-deviance interventions moving forward, research into the effectiveness of each of these strategies within the context of intervention implementation is essential. There is a need for criminological research to develop robust, evidence-based interventions. In order to achieve this, prevention initiatives and interventions should be designed to address empirically validated risk factors. Furthermore, these interventions must be rigorously evaluated to determine whether they are effective at preventing deviance and to ensure that no adverse consequences occur as a result of the initiative.

INTRODUCTION

Digital technologies, and particularly the internet, play a significant and increasingly central part in adolescent life. This is particularly evident in Australia, where adolescents use the internet more than any other age group (ABS 2016; Green et al. 2011). This digital technology use involves specialised and diverse practices, including using multiple, always-connected devices in an increasing number of places, more time spent online, less online supervision and greater variety in terms of the types of things done online (Nansen et al. 2012). The scale and extent of digital penetration into the everyday lives of young people is immensely important from a policy perspective. The increased exposure to a multitude of digital technologies and use as routine activities presents new opportunities and incentives for engagement in various forms of delinquency, challenging existing practices aimed at prevention and intervention (Williams 2006; Yar 2005).

While such topics as eSafety and cyber-security targeting young people represent a major policy and investment focus in Australia and in other countries (Commonwealth of Australia 2016; Nansen et al 2012), there is only limited empirical evidence guiding these strategies and approaches (Shin & Lwin 2016). At present, little systematic attention is being paid to the specific digital settings and contexts in which cyber-deviance occurs. As a result, many of the preventative programs developed or recommendations made are not necessarily evidence-based. Moreover, such initiatives also tend to ignore the role of the perpetrator (who can often displace to new targets, methods or forms of deviance) and place the onus on victims to protect themselves. Researchers, practitioners, and policymakers are now seeking more effective ways to prevent young people from engaging in a myriad of risk-taking behaviours online and to practically prevent or facilitate desistance from cyber-deviance. At present, they face a largely undeveloped body of evidence guiding practice. Identifying and articulating evidence-based approaches to developing effective interventions for young people is critical due to the increasingly serious social and economic harms associated with increasing levels of online fraud, image-based abuse, unauthorised computer access, cyber stalking, bullying and harassment (Brewer et al. 2018; Cale et al. 2019; Livingstone et al. 2010; 2011).

Designing evidence-based approaches to prevention online

Before developing any type of preventative measure, it is crucial to first consider when the intervention would be the most appropriate - acknowledging that this may be different from one form of deviance to the next. Determining where and how to direct an intervention can be based on several factors, including characteristics of the delinquent behaviour and the perpetrator group, as well as more practical considerations such as resources. Importantly, much research (e.g. Andrews & Bonta 2010; Andrews et al. 1990; Bonta & Andrews 2017; Dowden & Andrews 1999; Koehler et al. 2013) suggests the development of effective interventions relies on the *accurate identification of factors known to contribute to deviance*.

A substantial body of research has identified these factors associated with deviance - at least for offline environments. While such factors vary somewhat across different delinquent populations, there is substantial overlap between categories, and correlates for delinquent behaviour show many similarities for specific forms of perpetration (Bonta & Andrews 2017). The best-validated risk factors for delinquent behaviour include a range of individual factors such as: gender and age, substance abuse, low

educational achievement/unemployment, antisocial personality patterns (i.e. impulsivity, poor problem-solving), antisocial cognition (i.e. attitudes/values/beliefs that promote delinquent behaviour such as lack of empathy, pro-crime justifications, and anti-law attitudes); social factors including unstable living arrangements, exposure to delinquent peers, and lack of structured prosocial leisure activities; and family factors including coming from a low socio-economic status home, abuse and neglect, poor parental mental health, parental criminal history, and parenting practices (i.e. disciplinary styles, autonomy and affection, and supervision); (for reviews see Cottle et al. 2001; Gendreau et al. 1996; Lipsey & Derzon 1998; Murray & Farrington 2010).

The literature broadly categorises such risk factors as being either static or dynamic. Static risk factors, such as age or biological sex, are unaffected by behavioural prevention and intervention strategies (Farrington 2007). On the other hand, dynamic risk factors, such as peer rejection or behavioural regulation, are potentially amenable to exogenous influences. Prevention and intervention strategies target an array of dynamic risk factors in order to reduce the risk of future delinquency. Identifying vulnerable people as early as possible is key for preventing the cumulative adversities and negative outcomes associated with these factors (Loeber et al. 2003).

In the absence of any corrective intervention, dynamic risk factors that emerge in early childhood, particularly those relating to child behavioural development and upbringing, tend to be relatively stable across time. For example, an array of longitudinal research has found that adolescent delinquents are more likely to experience risk-taking behaviours (Coyne & Wright 2014; Diamond 2016), conduct problems (Moffitt 2018; Storvoll & Wichstrom 2003), hyperactivity (Kuntsi et al. 2005), poor emotional regulation (Prenoveau et al 2011), impaired peer relationships (Bornstein et al. 2010), and adverse parenting (Dallaire & Weinraub 2005; Holden & Miller 1999); all of which are likely to first emerge in childhood. Dynamic risk factors that are relatively stable across time tend to have amongst the strongest influence on the risk of offline delinquency and may also be a precursor for serious and persistent antisocial behaviours (Farrington, 2010; Moffitt et al. 1996). Fortunately, given that these stable risk factors often first manifest at an early age, vulnerable young people can be prospectively identified early-in-life, and subsequently prioritised for indicated prevention programs.

When it comes to understanding cyber-deviance, however, the evidence base regarding risk factors with relevance to prevention is far less developed, particularly as it pertains to young people. In recent years, researchers have hypothesised that there may be distinctive and divergent criminogenic factors at play for cyber-deviance, when compared to offline forms of deviance (Goldsmith & Brewer 2015). This work argued that features of online environments (i.e. relative anonymity, deterritorialisation, synchronous and asynchronous encounters with known and also unknown others), can have profound implications for how adolescent delinquency arises, and can therefore make the digital environment a hazardous place from risk management and mitigation perspective (Goldsmith & Brewer, 2015). Recent studies have begun to account for these criminogenic properties and understand cyber-deviance as driven by not only individual (and idiosyncratic) attributes, but also as a function of *exposure* to digital technologies, sites and services, and the interactional opportunities afforded as a consequence (e.g. Brewer et al. 2018; Cale et al. 2019). This body of work suggests that in order to fully understand the risk factors online, both idiosyncratic and exposure measures must be accounted for.

This report aims to identify the time-stable idiosyncratic and interactional risk factors that are associated with cyber deviance in Australia. To do so, this report draws upon a sample of South Australian adolescents to examine their engagement in a variety of different types of cyber-deviance that have been identified in the research literature and contemporary policy discussions as being particularly relevant to young people (e.g. see https://www.esafety.gov.au/key-issues). These include: (1) cyber-bullying or abuse, (2) sexting, (3) image-based sexual abuse, (4) unauthorised access (hacking), (5) online fraud, (6) digital piracy, (7) cyber-hate, and (8) cyber-violence. Developing a nuanced understanding of these risk factors associated with and across each of these forms of cyber-deviance provides essential evidence that can be used in the development of targeted interventions in these areas.

METHODOLOGY

This report draws upon data collected from a survey conducted amongst a sample of 14-17 year olds enrolled at an urban South Australian secondary school (n=327). The paper-based survey was administered during class time, and asked participants to self-report their engagement with the aforementioned eight forms of cyber-deviance. In the context of this report, 'cyber-bullying and abuse' refers to searching for, sending, or sharing information with other people with the express purpose of making them feel uncomfortable. 'Sexting' reflects receiving sexual content of someone known to the participant, as well as sharing sexual content featuring themselves. 'Image-based sexual abuse' involves the sharing of someone else's sexual content without their consent. 'Unauthorised access' (or hacking) refers to accessing other people's devices or accounts without their permission. 'Online fraud' includes such activities as purchasing or selling illegal items online or tricking people into sending information or money. 'Digital piracy' refers to viewing, sharing or downloading of digital content that should have been paid for, but was not. 'Cyber-hate' refers to participant engagement with discriminatory content online and is separated into passive participation (viewing) and active participation (sharing). Finally, 'cyber-violence' again includes passive participation (viewing) or active participation (sharing) with content involving serious violence against people whom the student may or may not know. A complete list of the individual items included within each risk-taking type is available at Appendix 1.1.

A number of highly validated and reliable idiosyncratic risk factors were included in this study which have been found to reliably gauge a participant's emotional symptoms, conduct problems, hyperactivity/inattention, peer relationship problems, prosocial behaviour (measures derived from the *Strengths and Difficulties questionnaire* [SDQ], see Appendix 1.2), propensity for risk-taking (measures derived from the *National Longitudinal Survey of Youth, Children and Young Adults*, see Appendix 1.3), and perceptions of parental supervision, autonomy and discipline (measures derived from the *Parental Authority Questionnaire*, see Appendix 1.4). In addition to the time-stable factors listed above, and to account for digital contexts, this study incorporates measures of participant online exposure. Measures of routine, social and specialised exposure were constructed using previously validated measures derived from the *South Australian Digital Youth Survey,* see Appendix 1.5).

STUDY SAMPLE CHARACTERISTICS

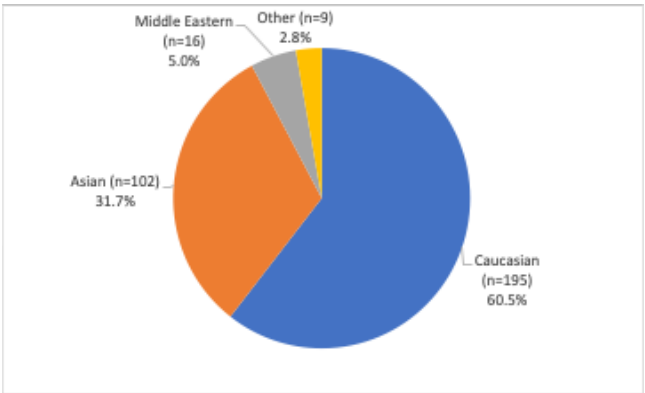
Year-level

Of the 327 students who participated in this survey, 46 (14.1%) were enrolled in Year 10, 143 (43.5%) were in Year 11, and 138 (42.2%) were in Year 12. The below analysis distinguishes between grades (instead of age) in order to account for variations in student characteristics, such as peer influences or education level, attributed to shared temporal experiences (i.e., year level).

Gender

Figure 1 shows that females (59.7%) were slightly overrepresented in the sample, as compared to 39.4% (n=129) male. Three (0.9%) students left the gender question blank.

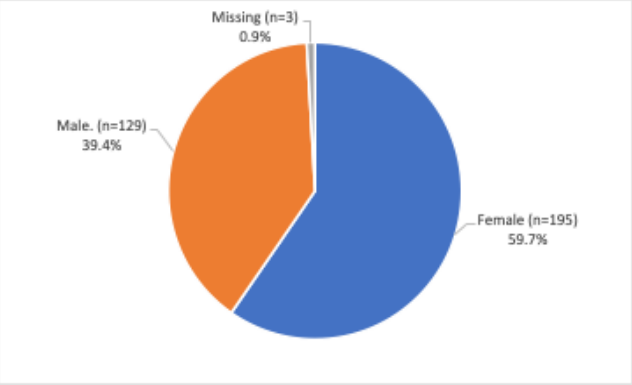
Figure 1: Gender



Ethnicity

Figure 2 shows that the majority (60.5%) of participants self-identified as being Caucasian. Approximately one third (31.7%) identified as Asian, 5.0% (n=16) identified as Middle Eastern, and 2.8% (n=9) as coming from another background. No participant in this sample identified as being Aboriginal and/or Torres Strait Islander.

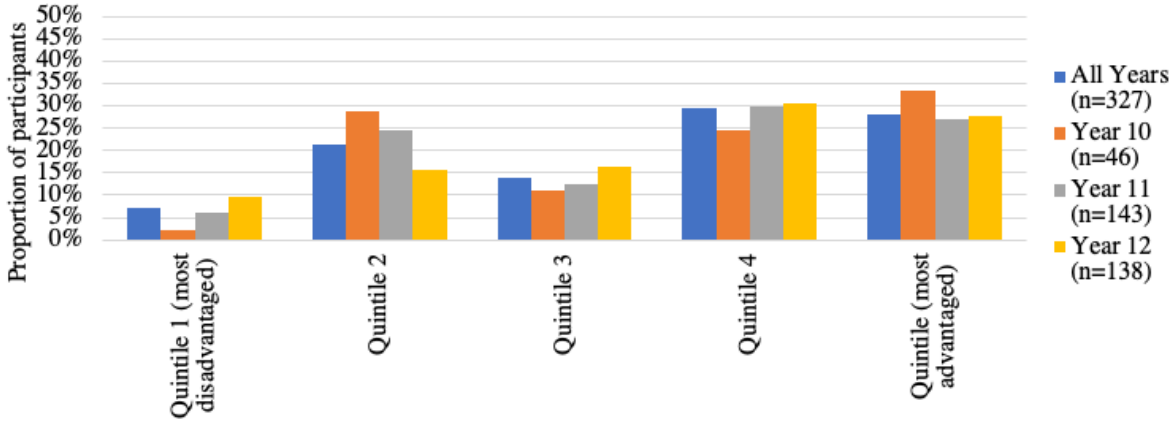
Figure 2: Ethnicity



Socioeconomic status

Figure 3 presents information about participants socioeconomic status – using the Australian Bureau of Statistics' *Socioeconomic Indexes for Areas* (SEIFA). SEIFA indexes the average income and employment status of individuals living within geographical areas defined by postcode. SEIFA quintiles were derived from the 2015 Australian census data, and range from most disadvantaged (quintile 1) to most advantaged (quintiles 5). This graph shows the distribution across SEIFA quintiles for the overall sample, which skews slightly toward being more advantaged.

Figure 3: Socioeconomic status by quintile

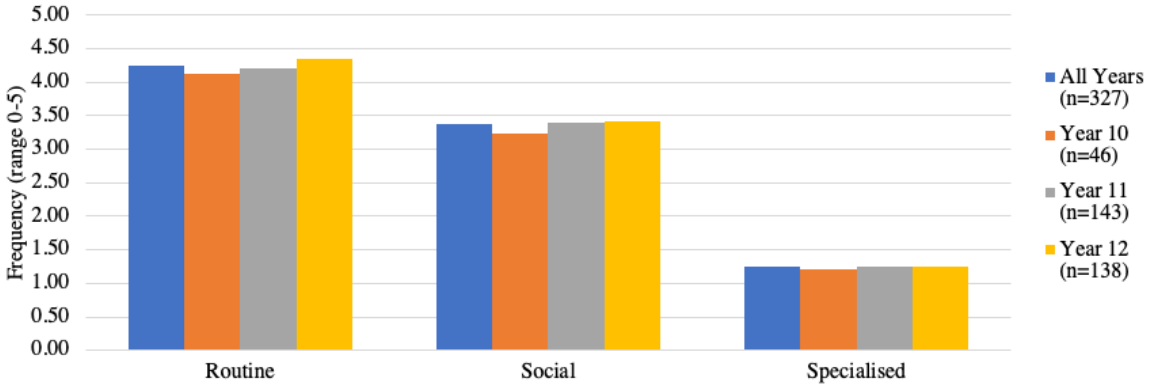


KEY RESULTS

Understanding the nature of adolescent online exposure

Figure 4 shows the frequency of three broad types of online activities that participants were exposed to. These activities were classified into three groups including: (1) routine exposure (e.g. using search engines, email, instant messaging, watching videos and viewing images outside of social media); (2) social exposure (e.g., browsing social media, sharing photos and videos on social media websites); and, (3) specialised exposure (e.g. creating websites, file sharing, browsing or posting to web forums, coding, online banking, using anonymisation software) (see Appendix 1.5 for the procedures used to derive these categories). Frequency was measured on a five-point Likert scale ranging from 0=Never to 5=Several times a day. The results show that, on average, students reported most frequently experiencing routine exposure, followed by social and specialised exposure.

Figure 4: Average frequency of online exposure



Understanding the prevalence of adolescent cyber-deviance

Figure 5 details the proportions of participants who reported engaging in different forms of cyber-deviance. The labels on the x-axis represent the eight forms of cyber-deviance considered in this study, whilst the y-axis represents the proportion of students involved. More than half of the sample in this study engaged in various forms of cyber-deviance, including passive engagement in cyber-hate (75.8%), digital piracy (65.7%), and passive engagement in cyber-violence (61.2%). Less common was unauthorised access (32.4%), sexting (27.2), cyber-bullying (16.5%), active engagement in cyber-hate (15.6%), online fraud (12.5%), active engagement in cyber-violence (11.0%) and image-based abuse (2.8%). Only 4.3% of participants reported abstaining from any such cyber-deviance.

Figure 5: Engagement in different types of cyber-deviance

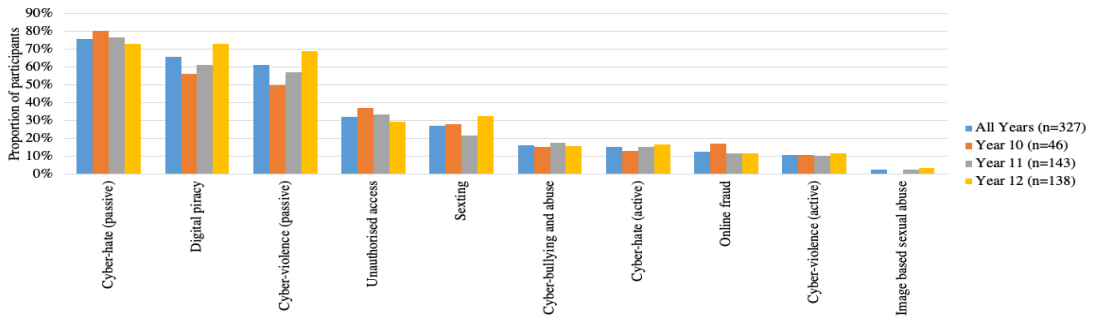


Figure 5 also shows that the prevalence of participation varies by grade. Compared to their younger counterparts, a greater proportion of older participants engaged in digital piracy, sexting, and passive cyber-violence. Conversely, a greater proportion of younger participants engaged in passive cyber hate and unauthorised access, although these differences were not statistically significant.

Identifying factors associated with cyber-deviance

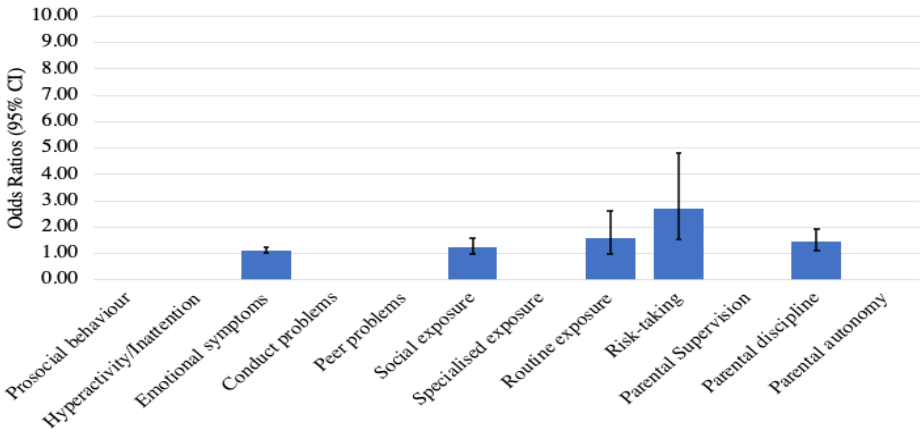
This section examines the risk factors that are associated with each type of cyber-deviance outlined above. In all analyses, we control for static factors (student gender, residential SEIFA, and school grade), which are not amenable to potential intervention strategies.

Cyber-hate

For the purposes of this study, cyber-hate is separated into two classes, based on their unique properties: *Passive participation* and *active participation.*

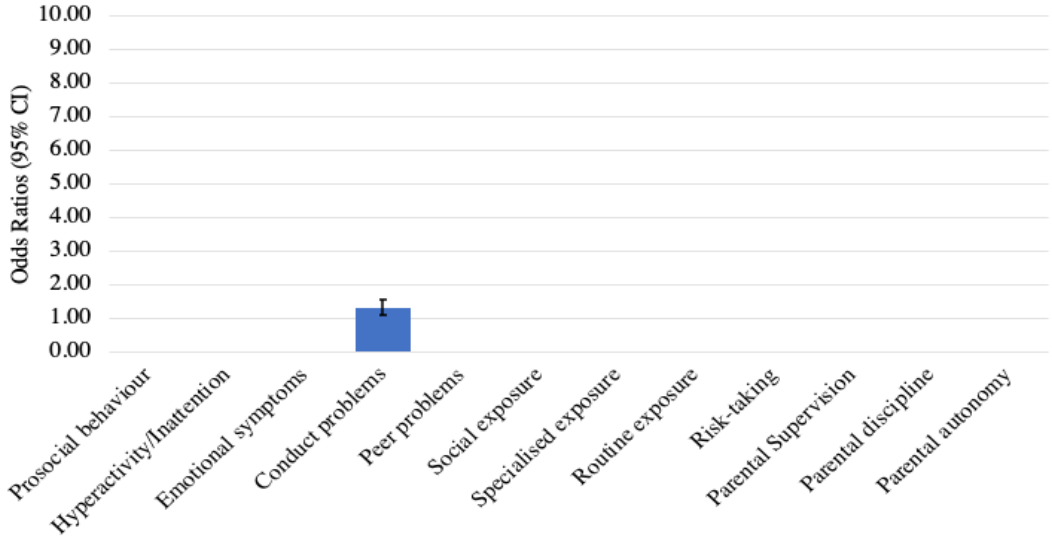
Passive participation in cyber-hate represents the most prevalent form of cyber-deviance reported by participants, with more than three-quarters (75.8%) of the sample engaging in these activities (Figure 5, above). The proportion of participants passively engaging in cyber-hate was slightly higher amongst younger participants: 80.4% amongst Years 10s, 76.9% for Year 11s and 73.2% for Years 12s (Figure 5, above). Figure 6 shows there are five risk factors associated with passive forms of cyber-hate: emotional symptoms, propensity for risk-taking, parental discipline and frequency of engagement in routine tasks and social tasks online. A participant's propensity for risk-taking was the most important factor. That is, for every unit increase in a participant's propensity for risk-taking (i.e. their score on the scale increases by 1), the likelihood of passively participating in cyber-violence increases 172%. By comparison, the odds of passively engaging in cyber-hate increased considerably for every one unit increase in disciplinary parenting practices (i.e. being stricter) (45%), reported emotional symptoms (12%), and routine exposure (60%) and social exposure (22%). These results show that there is overlap with a participant's propensity for risk-taking, the degree of exposure to online sites and services (particularly routine and social activities), parental disciplinary measures, as well as the adolescent's emotional symptoms (see Appendix 2, Table 1).

Figure 6: Factors associated with passive participation in cyber-hate



By comparison, relatively few students (15.6%) *actively* participated in cyber-hate, through the sharing of violent content online. As illustrated in Figure 5 (above), the proportion of students who engaged in this act was relatively consistent across Year 10 (13.0%), Year 11 (15.4%), and Year 12 (16.7%). Figure 7 shows that there was only a single risk factor that was associated with active participation with cyber-hate: conduct problems. These findings diverge from those identified for *passive* engagement in cyber-hate, in that parenting practices (discipline), exposure factors (routine and social tasks), and propensity for risk-taking did not come into play, and alternate measures of behavioural functioning (conduct problems versus emotional symptoms) proved significant. Closer examination of this single risk factor reveals that its potential impact on active participation in cyber-hate is marginal - that is, the likelihood of actively participating in cyber-hate increased by 4% for each unit increase in the conduct problems scale completed by the participant (see Appendix 2, Table 1).

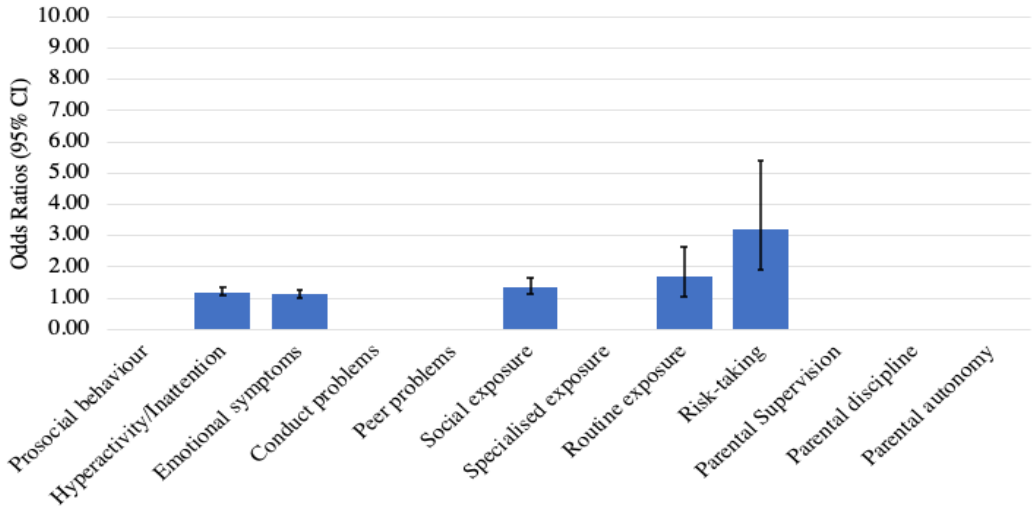
Figure 7: Factors associated with active participation in cyber-hate



Cyber-violence

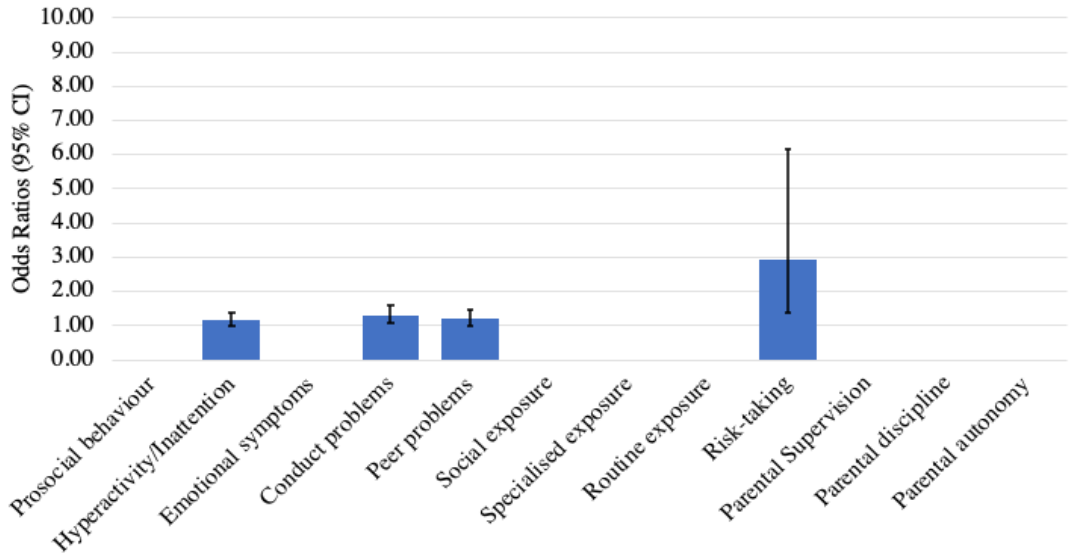
As was the case for cyber-hate, cyber-violence is separated into two classes for this study due to their unique properties: *Passive participation* and *active participation*. When it comes to *passive participation in cyber-violence,* the majority of participants indicated that they had viewed violent content online (Figure 5, above). A significantly greater proportion of these students were in Year 12 (68.8%), followed by Year 11 (57.3%), and Year 10 (50.0%). Figure 8 shows that there are five risk factors associated with passive forms of cyber-violence: hyperactivity, emotional symptoms, propensity for risk-taking and frequency of engagement in routine social tasks online. The most substantial factor is propensity for risk-taking. That is, for every unit increase in a participant's propensity for risk-taking, the likelihood of passively participating in cyber-violence increases 221%. Comparatively, the likelihood of engaging in online fraud increased considerably for every unit increase in hyperactivity (20%), emotional symptoms (13%), and engagement routine (69%) and social tasks (37%) (see Appendix 2, Table 1). These results show that there is overlap with a participant's propensity for risk-taking, the types of things they do online (particularly routine and social activities), as well as some forms of behavioural functioning (hyperactivity, conduct and peer problems). Parenting qualities were not significant when it came to passive participation in cyber-violence.

Figure 8: Factors associated with passive participation in cyber-violence



As for *Active participation in cyber-violence,* approximately one in ten (11.0%) students indicated that they had shared violent content online, with a consistent proportion of students across Year 10 (10.9%), Year 11 (10.5%), and Year 12 (11.6%). Figure 9 shows that four factors were associated with active engagement in cyber-violence. The most important of these factors was a participant's propensity for risk-taking, whereby each one unit increase was associated with a 221% increase in the likelihood of passively engaging in cyber-violence. Likewise, various behavioural functioning factors were associated with passive cyber-violence, with the likelihood of engagement increasing for each additional unit increase in hyperactivity (17%), conduct problems (29%) and peer problems (21%) (see Appendix 2, Table 1). These results diverged from passive engagement with cyber-violence, in that no significant associations were found with any situational factors, whilst different behavioural functions factors also came into play. In addition, the relationship between conduct problems and an increased likelihood of active engagement in cyber-violence is also mirrored in the case of active engagement of cyber-hate (see Figure 7, above).

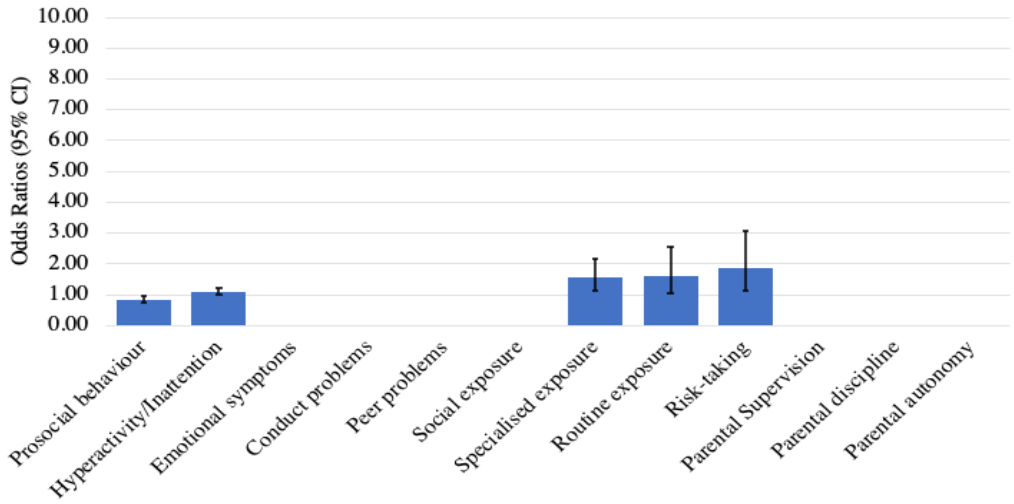
Figure 9: Factors associated with active participation in cyber-violence



Digital piracy

The majority of the participants in this study indicated they had engaged in digital piracy (65.7%), the proportion of whom was greatest for Year 12s (73.2%), followed by Year 11s (61.5%), and Year 10s (56.5%). Figure 10 (below) shows that five factors were significantly associated with digital piracy. Specifically, for every unit increase in a participant's propensity for risk-taking, participants were 87% more likely to engage in digital piracy. Elsewhere, the likelihood also increased by 62% for those more frequently experiencing routine online exposure, and 55% for those experiencing more frequent specialised exposure. Finally, the likelihood also increased by 10% for each additional unit increase relating to hyperactivity/inattention. By contrast, the odds of engaging in digital piracy were 18% *lower* among students reporting higher levels of prosocial behaviour (see Appendix 2, Table 1).

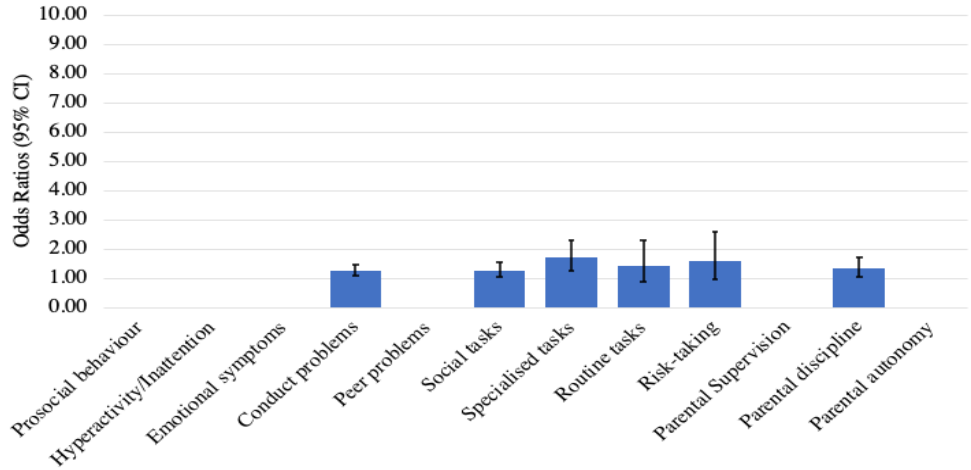
Figure 10: Factors associated with digital piracy



Unauthorised access or hacking

Just under one-third of students (32.4%) had engaged in the unauthorised access of someone's device or online account. The proportion of engagement in this activity across year levels of which was relatively consistent across Years 10 (37.0%), 11 (33.6%), and 12 (29.7%). As demonstrated in Figure 11, five factors were associated with increased likelihood of engaging in unauthorised access (or hacking). Situational factors were particularly relevant to hacking, with the likelihood of an adolescent engaging in hacking increasing for every one unit increase in their frequency of routine (41%), social (27%) and specialised (69%) online exposure. A participant's propensity for risk-taking was also found to be associated with hacking behaviours, with the likelihood of engagement increasing by 58% for every one unit increase on the risk-taking scale. In addition, participants who scored higher on the conduct problem scale were more likely to engage in hacking by 27% (per per unit increase), as were participants who experienced greater paternal discipline (33% per unit increase) (see Appendix 2, Table 1).

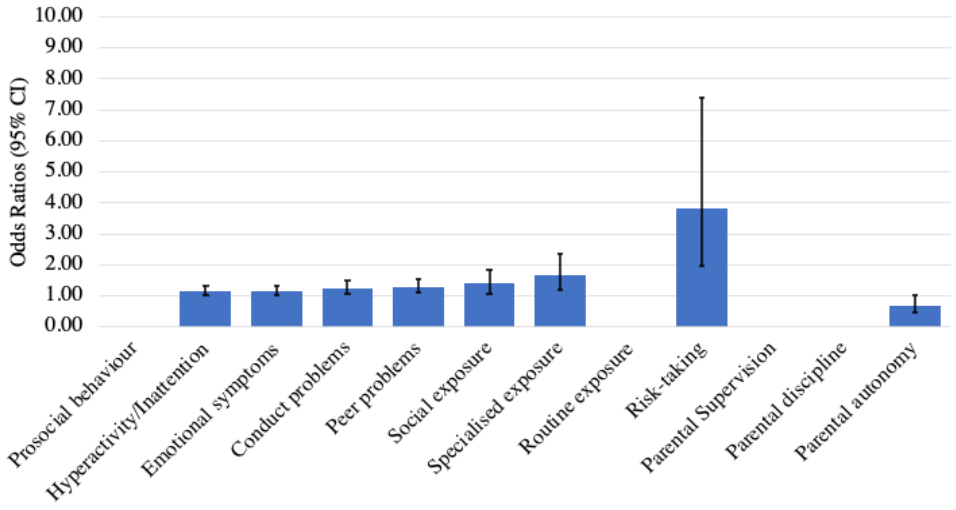
Figure 11: Factors associated with unauthorised access



Cyber-bullying and abuse

Comparatively few participants (16.5%) reported that they had engaged in cyber-bullying or abuse over the past year. The proportion of students who had reportedly engaged in this behaviour were similar across Years 10 (15.2%), 11 (17.5%), and 12 (15.9%). Figure 12 (below) shows that eight factors were significantly associated with cyber-bullying and abuse. Foremost, for every one-unit increase in a participant's propensity for risk-taking, the likelihood of engagement in cyber-bullying increased by 282%. In addition, the likelihood of engagement in cyberbullying also increased with each additional unit increase in behavioural functioning reported by the participant, including peer problems (30%), conduct problems (25%), hyperactivity (17%) and emotional problems (15%). Further, increased frequency in online exposure increased the likelihood of engaging in cyber-bullying, including through social (41% per unit increase) and specialised exposure (67% per unit increase). By contrast, participants reporting greater being endowed with greater levels of autonomy from parents were 45% *less* likely (per unit decrease) to engage in cyber-bullying and abuse (see Appendix 2, Table 1). When considered together, these results demonstrate the multifarious behavioural functioning, parental and exposure factors underpinning cyber-bullying.

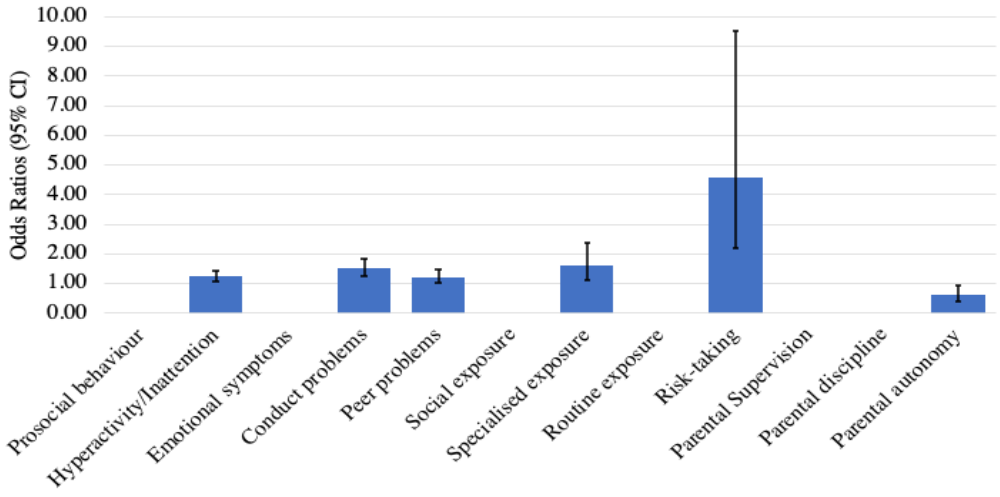
Figure 12: Factors associated with cyber-bullying and abuse



Online fraud

A small proportion of the participants in this study (12.5%) had reportedly engaged in online fraud during the past year. As noted in Figure 5 (above), the proportion of students engaging in this behaviour did not significantly differ between Grade 10 (17.4%), Grade 11 (11.9%), and Grade 12 (11.6%). Figure 13 (below) indicates that there are six factors associated with online fraud: hyperactivity/inattention, conduct problems, specialised exposure, and propensity for risk-taking. The most significant factor for online fraud is propensity for risk-taking. More specifically, for every unit increase in a participant's propensity for risk-taking, the likelihood of participating in online fraud increases 370%. Comparatively, the likelihood of engaging in online fraud increased considerably for every unit increase in hyperactivity (25%), conduct problems (54%), peer problems (23%) and specialised online exposure (62%). Conversely, for every one-unit increase in autonomy endowed by parents, the likelihood of engaging in online fraud decreased by 38%. These results show that there is overlap with a participant's propensity for risk-taking, the types of experiences they have online (specialised exposure), parenting styles (particularly parental autonomy), as well as some behavioural functioning (hyperactivity, conduct and peer problems) (see Appendix 2, Table 1).

Figure 13: Factors associated with online fraud



Sexting

During the past 12 months, more than a quarter of participants (27.2%) reported engaging in sexting. Figure 5 (above) shows that there was a slight degree of variation in the prevalence of sexting amongst participants across year levels, being reported by over a quarter (28.3%) of year 10s (28.3%), about one-in five year 11s (21.7%) and nearly one-third of year 12s (32.6%). Figure 14 (below) shows that there are eight stable risk factors associated with sexting, the most significant of those again being a participant's propensity for risk-taking. That is, for every one-unit increase in a participant's propensity for risk-taking, the likelihood of engaging in sexting increases by 199%. Elsewhere, the likelihood of a participant engaging in sexting also increased for every unit increase in hyperactivity (13%), emotional symptoms (11%), conduct problems (23%), prosocial behaviour (17%), parental autonomy (1%), frequency of social (47%) and specialised exposure (38%). These results again show that there is overlap with a participant's propensity for risk-taking, the types of experiences the have online (particularly social and specialised exposure), distinct parenting styles (particularly parental autonomy), as well as their behavioural functioning (engaging in prosocial behaviours, hyperactivity, exhibiting emotional symptoms and having conduct problems) (see Appendix 2, Table 1).

Figure 14: Factors associated with sexting

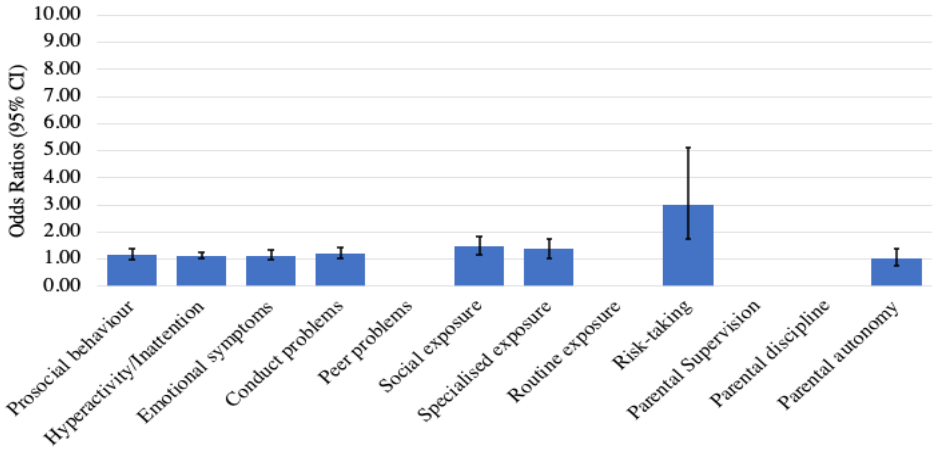
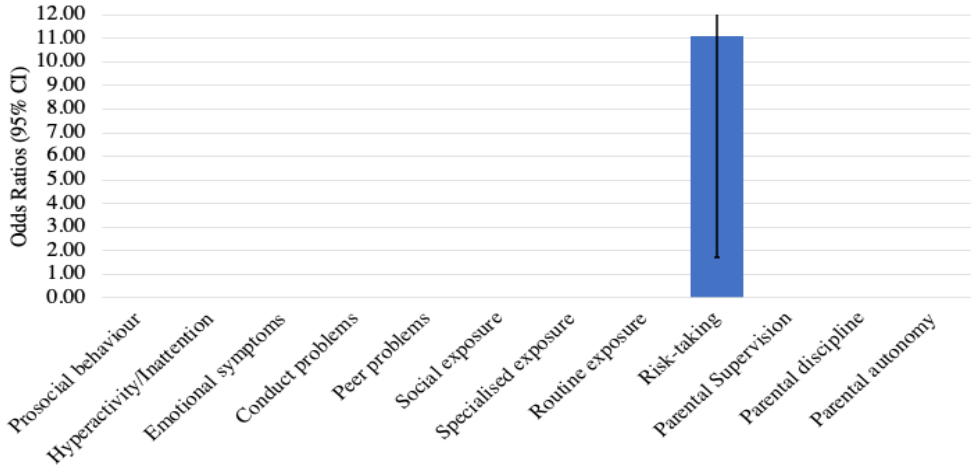


Image-based sexual abuse

Only a small proportion of participants (2.8%) reported engaging in image-based sexual abuse. No Year 10s engaged in this behavior, whilst very few Year 11s (2.8%) and slightly more Year 12s (3.6%) reported engagement (Figure 5, above). Figure 15 shows that propensity for risk-taking was the only significant risk factor associated with image-based sexual abuse. That is, for every one-unit increase in a participant's propensity for risk-taking, the likelihood of a respondent engaging in image-based abuse increased by a factor of 10 (1001%) (see Appendix 2, Table 1).

Figure 15: Factors associated with image-based abuse



Summary of findings

When considered together, these results depict several important trends when it comes to adolescent engagement in cyber-deviance. First, all of the risk factors pertaining to behavioural functioning widely affected cyber-deviance across nearly all forms. More specifically, problems linked with hyperactivity and inattention were the most pervasive, and were found to be associated with an increased likelihood of participants engaging in digital piracy, cyber-bullying, online fraud, sexting, as well as passive and active forms of cyber-violence. Conduct problems were also widespread and were found to be associated with an increased likelihood for engagement in hacking, cyber-bullying, online fraud, sexting and active participation in cyber-hate. Likewise, prevalence of emotional problems was also associated with an increased likelihood of adolescent engagement in cyber-bullying and sexting, as well as passive forms of cyber-hate and cyber violence. In addition, having peer problems was associated with an increased likelihood of engaging in cyber-bullying and fraud, whilst exhibiting more prosocial behaviours was associated with an increased likelihood of engagement in digital piracy and sexting. The only form of cyber-deviance not associated with any behavioural function factor was image-based sexual abuse, although the association between this activity and an adolescent's propensity for risk-taking was especially powerful. Elsewhere, an adolescent's increased propensity for risk-taking proved to be associated with engagement in all forms of cyber-deviance, except for active participation in cyber-hate.

Several parenting practices were also found to be associated with an increased likelihood of adolescent engagement in some forms of cyber-deviance. In particular, higher levels of parental autonomy were associated with an increased likelihood of adolescent engagement in sexting, but a decrease in cyber-bullying and online fraud. Likewise, higher levels of parental discipline are associated with an increased likelihood of engagement in hacking and passive forms of cyber-hate. Notably, the degree of parental supervision experienced by participants had no observed association with any form of cyber-deviance, whilst piracy, image-based sexual abuse, active participation in cyber-hate, and passive and active participation in cyber-violence were not associated with any discrepancies in parenting styles.

The types of experiences that young people had whilst online (i.e. online exposure) were also found to be associated with an increased likelihood of engagement in various forms of cyber-deviance. For example, increased frequency of routine exposure was associated with an increased likelihood of engagement in hacking, digital piracy, and passive participation in cyber-hate and cyber-violence. Increased social exposure was associated with an increased likelihood for engagement in a different configuration of cyber-deviance types: overlapping with engagement with routine exposure, which was also associated with hacking, and passive engagement with cyber-hate and cyber-violence, but also being associated with cyber-bullying and sexting. Increased specialised exposure was also associated with an increased likelihood of engagement in overlapping forms of cyber-deviance, including hacking, digital piracy, cyber-bullying and sexting, as well as being the sole situational factor found to be associated with an increased likelihood of engagement in online fraud.

IMPLICATIONS FOR POLICY AND PRACTICE

Developing a nuanced understanding of the risk factors associated with each form of cyber-deviance provides an evidence base for the development of targeted interventions. It is imperative that interventions address risk factors from a number of domains, as it is evident from this study that individual-level risk factors alone do not predict engagement in cyber-deviance. Consequently, intervention programs designed to target risk factors within a single domain are unlikely to effectively address cyber-deviance. Furthermore, the efficacy of cyber-deviance interventions is reliant on the identification of risk factors which have been empirically shown to correlate with the problematic behaviour (Andrews & Bonta 2010; Andrews et al. 1990; Bonta & Andrews 2017). This study demonstrated that a number of individual, technosocial and family factors interact to increase the propensity for cyber-deviance in adolescence. The practical and policy implications of these findings - for parents, schools, industry, law enforcement and other government sectors - will now be discussed.

Dynamic risk factors that are stable over time within a family context were found to be associated with several forms of cyber-deviance. Strict parental discipline was found to increase the likelihood of adolescent participation in unauthorised access and passive cyber-hate. In contrast, increased parental autonomy was found to decrease engagement in cyber-bullying and abuse, as well as online fraud. Given that parenting can have both positive and negative effects on adolescent cyber-deviance it is important that intervention programs endeavour to include parents in the design of their programs.

While some cyber-bullying interventions, for example, have been designed to include parents, the majority tend to focus on adolescent perpetrators and their immediate school environment (Gaffney et al. 2019). Parent training, in which parents are taught to minimise harsh discipline and emphasise positive parenting practices have been successful in decreasing conduct and attentional problems in children (Bjorknes et al. 2012; Hartman et al. 2003). We therefore suggest that it would be useful for researchers to consider incorporating some form of parental training or involvement in the design of relevant interventions, in order to educate, as well as address disciplinary issues and facilitate the development of positive parent-child relationships.

Measures of online exposure were important across the board in this study. In particular, specialised exposure was associated with the majority of cyber-deviance types. Criminogenic opportunities are more numerous in online spaces than they are in offline spaces, with individuals able to access illicit sites and systems from the safety of their homes (Brewer et al. 2018). The nature of online exposure can therefore influence the likelihood of adolescents accessing and engaging with illicit content online. The situational crime prevention (SCP) approach has potential for addressing these risk factors. The SCP approach is concerned with reducing opportunities for deviance by increasing the effort and risks, and decreasing the rewards associated with committing an offence (Clarke 1995). SCP techniques have proven effective for reducing offline offences, including robbery (Crow & Bull 1975; Scott et al. 1985), vandalism (Sloan-Howitt & Kelling 1990) and shoplifting (Farrington 1993). However, these techniques have not been extensively applied for the prevention of cyber-deviance. The application of SCP techniques for preventing cyber-deviance has primarily focused on three strategies: antivirus products, warnings and surveillance software (Brewer et al. 2019). The most successful of these strategies has been antivirus software, with the remaining two strategies producing mixed findings (Brewer et al. 2019). It might be expected that parental supervision would serve to increase the effort required to engage in cyber-deviance. Interestingly, this study found that parental supervision was not significantly associated with cyber-deviance. This emphasises the need for future research to ascertain how other SCP techniques could be effective at reducing cyber-deviance within an adolescent population, particularly given the potential this approach has to reduce criminogenic opportunities.

While it is important to understand the dynamic risk factors associated with engagement in different forms of cyber-deviance, the identification of commonly occurring risk factors is valuable as it enables the design of interventions to potentially reduce multiple forms of problematic behaviour. Designing interventions that target multiple risk factors, which have been shown to influence the likelihood for engagement in numerous forms of cyber-deviance is therefore more efficient than designing an intervention to target the risk factors for one form of cyber-deviance alone. This study found that propensity for risk-taking was a significant risk factor for every form of cyber-deviance, with the exception of active participation in cyber-hate. In addition, emotional, peer and conduct problems were found in almost half of the forms of cyber-deviance. It would be prudent to employ a strategy to target these risk factors, as they are commonly occurring across all forms of cyber-deviance.

A strategy which could potentially be suitable for addressing these risk factors could be to draw from social and emotional learning (SEL) programs, which aim to develop self-awareness, self-management, social awareness, relationship skills and responsible decision making (Greenberg et al. 2003). SEL programs have had considerable positive impact on improving social and emotional skills, attitudes, behaviour and academic performance as well as increasing self-control and fewer conduct problems in adolescents (Coelho & Sousa 2017; Durlak et al. 2011). Furthermore, the development of social and emotional skills has positive ramifications for behavioural functioning in adolescents (Coelho

& Sousa 2017). Given the significance of impulsive risk-taking as a risk factor across the board, SEL programs may be particularly valuable in reducing cyber-deviance. While few interventions have incorporated SEL components into their design, those who have evidenced a decline in cyber-bullying and aggression in participants (Espelage et al. 2015; Garaigordobil & Martinez-Valderrey 2018). The incorporation of SEL elements into intervention design has the potential to address several of the risk factors identified in this study.

This study has demonstrated the importance of considering time stable, dynamic risk factors in the design of interventions. The incorporation of SEL components, inclusion of parents and consideration of SCP techniques have been outlined as potential strategies for cyber-deviance interventions moving forward. However, research into the effectiveness of each of these strategies within the context of cyber-deviance interventions is highly underdeveloped. There is a need for criminological research to develop robust, evidence-based interventions and undertake a rigorous evaluation of these strategies to determine their efficacy in reducing cyber-deviance.

Building evaluations into an intervention's design and implementation

It is crucial to ensure that any prevention strategies or interventions (newly designed, or pre-existing) are effective, delivering value for money, and that there are no unforeseen or undesirable consequences (Hutchings & Holt 2017). In the same way that clinical trials are necessary to ensure that medicines are effective at preventing and treating diseases, cyber-deviance interventions should also be rigorously evaluated to determine whether interventions are effective at preventing deviance, or reducing recidivism. Through the collection of rich data such as was done in this report, it is possible to determine whether specific factors associated with an intervention have an impact on positive outcomes, as well as take stock of any other moderating effects.

Undertaking evaluations also provide other crucial insights that might otherwise not be immediately apparent. By way of example, Brewer and colleagues (2019) showed that some poorly designed cyber-deviance interventions show an association with *increased* anti-social activity (see also Grabosky 1996; McCord 2003; Sherman 1993; Welsh & Farrington 2001). The factors driving these trends are complex and multifaceted and may be a product of poor intervention planning or training, net-widening effects, peer contagion, or displacement among others. Researchers are still exploring and identifying the potential unintended outcomes for interventions designed to disrupt cyber-deviance (see further Hutchings et al. 2016; Moore & Clayton 2011; Soska & Christin 2015), and additional rigorous study is warranted.

Whilst it is outside the scope of this report to provide a detailed account of how to conduct evaluations, readers should consult the wealth of available resources on this topic (see, e.g., Cook & Campbell 1979; Ekblom & Pease 1995; Shaw et al. 2006, among others). Importantly, before embarking on this process, Brewer and colleagues (2019) flag that there are numerous potential challenges that researchers and practitioners are likely to confront when setting out to design evaluations. These include selecting appropriate study designs (preferably experimental or quasi-experimental designs); sourcing high quality data (either official records, self-report or observational data) that is collected both pre- and post-intervention, and for an adequate follow-up period, and being attentive to a variety of ethical considerations (for a detailed treatment of these aspects, see Brewer et al 2019, pp. 127-142).

APPENDIX 1: MEASURES

1.1 Cyber-deviance

Participants were asked if, in the last 12 months, they had "never", "less than weekly", "about once a week", "several times a week", "about once a day", or "several times a day", engaged in a series of cyber-deviance behaviours using either a desktop computer, laptop, tablet, or smartphone. Ten scales were used to measure distinct types of cyber-deviance (listed below). An indicator variable was created for each scale, indicating if participants had ever engaged in that type of behaviour over the last 12 months.

Online fraud

Online Fraud was measured via the following five items (α=.81): "bought anything that might be against the law", "sold anything that might be against the law", "tricked another person into sending you their personal information", "tricked another person into giving you money", and "tricked a business or organisation into sending you money, goods, or services".

Sexting

Sexting was measured by two items (α=.70): "seen sexual content (e.g., text, images, or videos) of someone you know" and "shared sexual content (e.g., text, images, or videos) of yourself".

Image-based sexual abuse

Image-based sexual abuse was measured by a single item: "shared sexual content (e.g., text, images or videos) of someone else without their consent".

Cyber-hate

In this report, we acknowledge the literature that distinguishes between passive and active forms of cyber-hate (e.g. see Jacks & Adler 2015).

Passive participation in cyber-hate (α=.74) was measured by asking students if they had "seen content (text, images or video) making fun of someone you know because they were different", "seen content (text, images or video) making fun of someone you don't know because they were different", and "seen content (text, images or video) making fun of a group of people because they were different".

Active participation in cyber-hate (α=.79) was measured by asking students if they had "shared content (text, images or video) making fun of a particular person because they were different" and "Shared content (text, images or video) making fun of a group of people because they were different".

Cyber-violence

Passive participation in cyber-violence was measured by three items (α=.77): “seen content (e.g., text, images, or videos) involving serious violence against someone you know”, “seen content (e.g., text, images, or videos) involving serious violence against someone you don’t know (not including movies, tv, or video games)”, and “seen content (e.g., text, images, or videos) involving serious violence against a group of people (not including movies, tv, or video games)”.

Active participation in cyber-violence was measured by two items (α=.79): “shared content (text, images or videos) involving serious violence against another person” and “shared content (text, images or videos) involving serious violence against a group of people”.

Digital piracy

Four items were used to measure participant engagement in *digital piracy* (α=.84): “listened to music that you think you should have paid for”, “watched a video that you think you should have paid for”, “downloaded software, games, or eBooks that you think you should have paid for”, and “shared music, videos, software, games, or eBooks with others that you think they should have paid for”.

Cyberbullying and abuse

Cyberbullying and abuse was measured by the following three items (α=.78): “searched for information online about someone that you could use to make them feel bad or scared”, “privately sent content (e.g., text, images or videos) to make someone feel bad or scared”, and “publicly shared content (e.g., text, images or videos) to make someone feel bad or scared”.

Unauthorised device access or hacking

Unauthorised device access was measured via the following four items (α=.86): “accessed another person's device (without their permission) to look at information, photos, videos or other files”, “accessed another person's device (without their permission) to add, delete or change information or other files”, “accessed another person's online account (without their permission) to look at information (messages, emails, etc), photos, videos, or other files”, and “accessed another person's online account (without their permission) to add, delete or change information/files”.

1.2 Behavioural functioning

The Strength and Difficulties Questionnaire (SDQ) is a widely validated measure of the behavioural, emotional, and social functioning of young people aged 4-17 years (Goodman, 1997). The SDQ includes 25 questions, with young people indicating their agreement to each item according to a three-point scale (not true, somewhat true, and certainly true). Scores were summed across the five items

for each scale, with higher scores indicating poorer functioning (except for the prosocial behaviour scale, where higher scores indicated better functioning).

Prosocial behaviour (α=.63) items are "I try to be nice to other people", "I usually share with others", "I am helpful if someone is hurt, upset or feeling ill", "I am kind to younger children", and "I often volunteer to help others.

Hyperactivity/Interaction (α=.76) items are "I am restless; I cannot stay still for long", "I am constantly fidgeting or squirming", "I am easily distracted", "I think before I do things" (reverse coded), and "I finish the work I am doing" (reverse coded).

Emotional Symptoms (α=.73) items are "I get a lot of headaches, stomach aches or sickness", "I worry a lot", "I am often unhappy, downhearted or tearful", "I am nervous in new situations", and "I have many fears; I am easily scared".

Conduct Problems (α=.51) items are "I get very angry and often lose my temper", "I usually do as I am told" (reverse coded), "I fight a lot", "I am accused of lying or cheating", and "I take things that are not mine".

Peer relationship problems (α=.53) items are "I am usually on my own", "I have one good friend or more" (reverse coded), "Other people my age generally like me" (reverse coded), "Other children or young people pick on me", and "I get on better with adults than with people my age".

1.3 Propensity for risk-taking

Propensity for risk-taking was measured using six items based on the propensity for risk-taking scale derived from the *National Longitudinal Survey of Youth, Children and Young Adults*. Participants used a four-point Likert scale (strongly disagree, disagree, agree, strongly agree) to indicate their agreement with the following six statements (α = .71): "planning takes all the fun out of things"; "I enjoy taking risks"; "I often get into trouble because I do things without thinking"; "I enjoy new and exciting experiences, even if it is a little frightening"; "life with no danger in it would be too dull for me", and; "I have to use a lot of self-control to keep out of trouble". Scores were averaged across the six items, with higher scores signifying lower self-control (range 1-4).

1.4 Parenting practices

Participants were administered eight questions asking them to indicate how often (i.e., never, rarely, sometimes, mostly, always) their parents engaged in the following parenting practices: "supervises your activities very carefully"; "expects you to do as you are told without explanation"; "watches everything you do"; "you are expected to do what you are told immediately"; "believes strict discipline is good for you"; "encourages you to play with other children"; "expects you to disagree with them if you think they are wrong", and; "encourage you to do your own thing".

Principal component analysis was conducted to reduce these eight items into discernible components reflecting types of parenting styles. Three components had an eigenvalue greater than one and collectively explained 70.52% of the total variance. The Kaiser-Meyer-Olkin statistic indicated that the data was suitable for factor analysis (KMO=.71), and the communalities for all items range from .48 to .85.

The first component (eigenvalue = 2.99; variance = 37.35%) had a rotated loading of two items: "supervises your activities very carefully" and "watches everything you do". These two items have a Cronbach's alpha score of .85 and a mean inter-item correlation of .74. This component was designated as *parental supervision,* with higher scores indicating more frequent parental monitoring of the child.

The second component (eigenvalue = 1.60; variance = 19.99%) had a rotated loading of three items: "expects you to do as you are told without explanation", "you are expected to do what you are told immediately", and "believes strict discipline is good for you". These three items have a Cronbach's alpha score of .78 and a mean inter-item correlation of .55. This component was designated as *strict parental discipline,* with higher scores indicating a greater propensity for parents to favour strict disciplinary attitudes.

The third component (eigenvalue = 1.06; variance = 13.27%) also had a rotated loading of three items: "encourages you to play with other children", "expects you to disagree with them if you think they are wrong", and "encourage you to do your own thing". These three items have a Cronbach's alpha score of .55 and a mean inter-item correlation of .30. This component was designated as *parental autonomy,* with higher scores indicating greater parental trust and communication.

1.5 Online exposure

Participants were administered 15 items regarding how often (i.e., never, less than weekly, about once a week, several times a week, about once a day, or several times a day) they engaged with the following activities online: "used search engines"; "browsed social media"; "listened to music"; "looked at photos or images outside of social media"; "sent instant messages"; "sent or received emails"; "watched videos or movies outside of social media"; "coded or wrote software"; "used software to hide identity"; "browsed or posted on an online forum"; "shared photos online"; "used online banking"; "worked on own website or created content to post online"; "shared videos online", and; "used file sharing or cloud syncing software".

Principal components analysis with three fixed factors was conducted to assess construct validity and reduce these 15 items into discernible components reflecting types of digital device use. The three components had an eigenvalue greater than one and explained 45.32% of the total variance. The Kaiser-Meyer-Olkin statistic indicated that the data was suitable for factor analysis (KMO=.72). Communalities for all items range from .39 to .86.

The first component (eigenvalue = 3.43; variance = 22.9%) had a rotated loading of three items: “browsed social media (Facebook, Instagram, Twitter, etc)”, “shared your photos online (including posting to social media or sending via messaging apps)”, and “ shared your videos online (including posting to social media, sending via messaging apps or video-calling)”. These three items have a Cronbach’s alpha score of .78 and a mean inter-item correlation of 0.51, which is optimal for scales with less than ten items (Briggs & Cheek, 1986). We refer to this three-item component as *social exposure.*

The second component (eigenvalue = 1.99; variance = 13.3%) had a rotated loading of six items: “browsed or posted to an online forum”, “used online banking to send or receive money”, “worked on your own website or created your own content to post online (outside of social media)”, “used file sharing or cloud syncing software (e.g. Dropbox, OneDrive, BitTorrent, etc)”, “coding or writing software”, and “used software to cover your tracks online”. These six items have a Cronbach’s alpha score of .65 and a mean inter-item correlation of 0.26. We label this six-item component as *specialised exposure.*

The third component (eigenvalue = 1.37; variance = 9.16%) also had a rotated loading of six items: “searched for information using search engines (Google, Wikipedia, etc)”, “sent and/or received emails”, “sent instant messages (SMS, iMessage, Facebook messenger, etc)”, “watched videos or movies (outside of your social media feeds)”, “looked at photos or images (outside of your social media feeds)”, “listened to music (Spotify, Apple Music, or MP3s that you downloaded)”. These six items have a Cronbach’s alpha score of .57 and a mean inter-item correlation of .19. We label this six-item component as *routine exposure.* Scores were averaged across the items for each of the three components, with higher scores indicating greater respective online use (range 0-5).

APPENDIX 2: TABLES

Table 1. Odds Ratios and 95% Confidence Intervals (OR [95% CI]) of the association between risk factors and types of cyber-delinquency among all students, adjusted for student gender, grade, and residential socioeconomic status (N=327)

Risk Factor	TYPE OF CYBER-DELINQUENCY									
	ONLINE FRAUD	SEXTING	IMAGE ABUSE	PASSIVE CYBER-VIOLENCE	ACTIVE CYBER-VIOLENCE	PASSIVE CYBER-HATE	ACTIVE CYBER-HATE	DIGITAL PIRACY	CYBER-BULLYING	HACKING
Prosocial	0.97 (0.80-1.18)	**1.17 (1.00-1.37)**	1.31 (0.78-2.18)	1.02 (0.90-1.17)	1.11 (0.89-1.38)	0.97 (0.83-1.13)	0.96 (0.81-1.15)	0.85 (0.73-0.98)	0.89 (0.75-1.05)	0.93 (0.81-1.06)
Hyperactivity	**1.25 (1.08-1.44)**	**1.13 (1.02-1.25)**	1.20 (0.85-1.68)	**1.20 (1.09-1.34)**	**1.17 (1.01-1.37)**	0.99 (0.89-1.10)	1.12 (0.98-1.27)	**1.10 (1.00-1.21)**	**1.17 (1.03-1.34)**	0.99 (0.89-1.09)
Emotional	1.12 (0.97-1.30)	**1.11 (1.00-1.23)**	1.08 (0.78-1.48)	**1.13 (1.02-1.25)**	1.09 (0.93-1.26)	**1.12 (1.00-1.25)**	1.12 (0.98-1.28)	1.07 (0.96-1.18)	**1.15 (1.01-1.31)**	1.05 (0.95-1.16)
Conduct	**1.53 (1.25-1.86)**	**1.23 (1.05-1.43)**	1.40 (0.95-2.08)	1.10 (0.94-1.29)	**1.29 (1.06-1.58)**	1.12 (0.94-1.34)	**1.32 (1.10-1.57)**	1.04 (0.89-1.22)	**1.25 (1.05-1.48)**	**1.27 (1.09-1.48)**
Peer problems	**1.23 (1.03-1.47)**	1.04 (0.90-1.19)	1.21 (0.83-1.76)	1.08 (0.95-1.24)	**1.21 (1.00-1.47)**	1.12 (0.96-1.31)	1.13 (0.95-1.33)	1.10 (0.96-1.27)	**1.30 (1.10-1.53)**	1.01 (0.89-1.16)
Social media	1.24 (0.93-1.65)	**1.47 (1.18-1.83)**	1.26 (0.67-2.37)	**1.37 (1.13-1.65)**	1.27 (0.94-1.72)	**1.22 (1.00-1.50)**	1.12 (0.87-1.44)	1.18 (0.98-1.42)	**1.41 (1.08-1.83)**	**1.27 (1.04-1.55)**
Advanced use	**1.62 (1.11-2.36)**	**1.38 (1.02-1.87)**	1.14 (0.52-2.53)	1.25 (0.93-1.69)	1.11 (0.73-1.67)	1.00 (0.72-1.39)	0.96 (0.65-1.39)	**1.55 (1.12-2.17)**	**1.67 (1.19-2.36)**	**1.69 (1.24-2.30)**
Routine use	1.51 (0.73-3.12)	1.49 (0.89-2.50)	0.64 (0.2 – 2.04)	**1.69 (1.07-2.64)**	0.97 (0.50-1.87)	**1.6 (1.00-2.6)**	1.6 (0.82-3.12)	**1.62 (1.03-2.54)**	1.46 (0.78-2.74)	1.41 (0.87-2.20)
Self-control	**4.57 (2.19-3.12)**	**2.99 (1.75-5.12)**	**11.10 (1.84-66.73)**	**3.21 (1.91-5.4)**	**2.93 (1.39-6.18)**	**2.72 (1.55-4.79)**	1.67 (0.87-3.18)	**1.87 (1.15-3.05)**	**3.82 (1.97-7.40)**	**1.58 (1.00-2.57)**
Parental supervision	0.87 (0.61-1.23)	0.95 0.74-1.21)	0.88 (0.41-1.91)	0.96 (0.76-1.2)	0.97 (0.68-1.39)	0.99 (0.77-1.28)	0.96 (0.71-1.31)	0.97 (0.77-1.22)	1.28 (0.96-1.71)	1.14 (0.91-1.44)
Strict discipline	1.06 (0.75-1.51)	1.2 (0.92-1.55)	1.10 (0.5-2.41)	1.22 (0.96-1.54)	1.26 (0.86-1.86)	**1.45 (1.11-1.91)**	0.86 (0.62-1.18)	1.1 (0.87-1.4)	1.27 (0.92-1.74)	**1.33 (1.04-1.72)**
Autonomy	**0.62 (0.41-0.95)**	1.01 (0.74-1.38)	0.54 (0.22-1.32)	0.87 (0.64-1.17)	0.83 (0.53-1.29)	0.96 (0.69-1.35)	1.02 (0.69-1.51)	0.96 (0.71-1.30)	**0.69 (0.47-1.00)**	0.97 (0.72-1.31)

REFERENCES

ABS 2016, *Census: Australian Bureau of Statistics says website attacked by overseas hackers,* viewed 11 June 2020, <http://www.abc.net.au/news/2016-08-10/australian-bureau-of-statistics-says-census-website-hacked/7712216>.

Andrews, D & Bonta, J 2010, 'Rehabilitating criminal justice policy', *Psychology, Public Policy, and Law*, vol.16, pp. 39–55.

Andrews, D, Zinger, I, Hoge, R, Bonta, J, Gendreau, P & Cullen, F 1990', 'Does correctional treatment work? A clinically relevant and psychologically informed meta-analysis', *Criminology*, vol.28, pp. 369–404.

Bjørknes, R, Kjøbli, J, Manger, T & Jakobsen, R 2012, 'Parent training among ethnic minorities: Parenting practices as mediators of change in child conduct problems', *Family Relations,* vol. 61, no. 1, pp.101-114.

Bonta, J & Andrews, D 2017, *The psychology of criminal conduct,* 6th edn, Routledge: New York, NY.

Bornstein, M, Hahn, C & Haynes, O 2010, 'Social competence, externalizing, and internalizing behavioral adjustment from early childhood through early adolescence: Developmental cascades', *Development and Psychopathology*, vol. 22, no. 4, pp. 717-735.

Brewer, R, Cale, J, Goldsmith, A & Holt, T 2018, 'Young people, the Internet, and emerging pathways into criminality: A study of Australian adolescents', *International Journal of Cyber Criminology*, vol. 12, no. 1, pp. 115-132.

Brewer, R, de Vel-Palumbo, M, Hutchings, A, Holt, T, Goldsmith, A & Maimon, D 2019, *Cybercrime prevention: Theory and applications,* Palgrave Macmillan: Australia.

Cale, J, Whitten, T, Brewer, R, de Vel-Palumbo, M, Goldsmith, A & Holt, T 2019, *South Australian digital youth survey research report: Year 1 results*, University of Adelaide, Adelaide.

Clarke, R 1995, 'Situational crime prevention', *Crime and Justice*, vol. 19, pp. 91–150.

Coelho, V & Sousa, V 2017, 'Comparing two low middle school social and emotional learning program formats: A multilevel effectiveness study', *Journal of Youth Adolescence*, vol. 46, pp. 656-667.

Commonwealth of Australia 2016, *Australia's cyber security strategy*, Department of the Prime Minister and Cabinet, Canberra.

Cook, T & Campbell, D 1979, *Quasi-experimentation: Design and analysis issues for field settings,* Houghton Mifflin: Boston, MA.

Cottle, C, Lee, R & Heilbrun, K 2001, 'The prediction of criminal recidivism in juveniles: A meta-analysis', *Criminal Justice and Behavior*, vol. 28, pp. 367–394.

Coyne, M & Wright, J 2014, 'The stability of self-control across childhood', *Personality and Individual Differences*, vol. 69, pp. 144-149.

Crow, W & Bull, J 1975, *Robbery deterrence: An applied behavioral science demonstration—Final report*, Western Behavioral Sciences Institute, La Jolla, CA.

Dallaire, D & Weinraub, M 2005, 'The stability of parenting behaviors over the first 6 years of life', *Early Childhood Research Quarterly*, vol. 20, no. 2, pp. 201-219.

Diamond, B 2016, 'Assessing the determinants and stability of self-control into adulthood', *Criminal Justice and Behavior*, vol. 43, no. 7, pp. 951-968.

Dowden, C & Andrews, D 1999, 'What works in young offender treatment: A meta-analysis', *Forum on Corrections Research*, vol. 11, pp. 21–24.

Durlak, J, Weissberg, R, Dymnicki, A, Taylor, R & Schellinger, K 2011, 'The impact of enhancing students' social and emotional learning: A meta-analysis of school-based universal interventions', *Child Development*, vol. 82, no. 1, pp. 405-432.

Ekblom, P & Pease, K 1995, 'Evaluating crime prevention', *Crime and Justice,* vol. 19, pp. 585–662.

Espelage, D, Low, S, Van Ryzin, M & Polanin, J 2015, 'Clinical trial of second step middle school program: Impact on bullying, cyberbullying, homophobic teasing, and sexual harassment perpetration', *School Psychology Review*, vol. 44, no.4, pp.464-479.

Farrington, D 1993, 'Understanding and preventing bullying' in M Tonry (eds), *Crime and justice: A review of research,* University of Chicago: Chicago, pp. 381-458.

Farrington, D 2007, 'Childhood risk factors and risk-focused prevention' *The Oxford Handbook of Criminology*', vol. 4, pp. 602-640.

Gaffney, H, Farrington, D, Espelage, D & Ttofi, M 2019, 'Are cyberbullying intervention and prevention programs effective? A systematic and meta-analytical review', *Aggression and Violent Behavior*, vol. 45, pp. 134-153.

Gendreau, P, Little, T & Goggin, C 1996, 'A meta-analysis of the predictors of adult offender recidivism: What works!', *Criminology*, vol. 34, no. 4, pp. 575–608.

Garaigordobil, M and Martínez-Valderrey, V 2018, 'Technological resources to prevent cyberbullying during adolescence: the cyberprogram 2.0 program and the cooperative cybereduca 2.0 videogame', *Frontiers in Psychology,* vol. 9, p.1-12.

Grabosky, P 1996, 'Unintended consequences of crime prevention', *Crime Prevention Studies*, vol. 5, pp. 25–56.

Goldsmith, A & Brewer, R 2015, 'Digital drift and the criminal interaction order', *Theoretical Criminology,* vol. 19, no. 1, pp. 112–30.

Green, L, Brady, D, Ólafsson, K, Hartley, J & Lumby, C 2011, 'Risks and safety for Australian children on the Internet', C*ultural Science Journal*, vol. 4, no. 1, pp. 1-73.

Greenberg, M, Weissberg, R, O'Brien, M, Zins, J, Fredericks, L, Resnik, H & Elias, M 2003, 'Enhancing school-based prevention and youth development through coordinated social, emotional and academic learning', *American Psychologist*, vol. 58, no. 6-7, pp. 466-474.

Hartman, R, Stage, S & Webster-Stratton, C 2003, 'A growth curve analysis of parent training outcomes: Examining the influence of child risk factors (inattention, impulsivity, and hyperactivity problems), parental and family risk factors', *Journal of Child Psychology and Psychiatry*, vol. 44, no. 3, pp. 388-398.

Holden, G & Miller, P 1999, 'Enduring and different: A meta-analysis of the similarity in parents' child rearing', *Psychological Bulletin*, vol. 125, no. 2, pp. 223-254.

Hutchings, A & Holt, T 2017, 'The online stolen data market: Disruption and intervention approaches', *Global Crime*, vol. 18, no. 1, pp. 11–30.

Hutchings, A, Clayton, R & Anderson, R 2016, 'Taking down websites to prevent crime', in 2016 APWG Symposium on Electronic Crime Research, IEE.

Jacks, W & Adler, J 2015, 'A proposed typology of online hate crime', *Open Access Journal of Forensic Psychology*, vol. 7, pp. 64-89.

Koehler, J, Lösel, F, Akoensi, T & Humphreys, D 2013, 'A systematic review and meta-analysis on the effects of young offender treatment programs in Europe', *Journal of Experimental Criminology*, vol. 9, pp. 19–43.

Kuntsi, J, Rijsdijk, F, Ronald, A, Asherson, P & Plomin, R 2005, 'Genetic influences on the stability of attention-deficit/hyperactivity disorder symptoms from early to middle childhood', *Biological Psychiatry*, vol. 57, no. 6, pp. 647-654.

Lipsey, M & Derzon, J 1998, 'Predictors of serious delinquency in adolescence and early adulthood: A synthesis of longitudinal research', in R Loeber & D Farrington (eds), *Serious and violent offenders: Risk factors and successful interventions*, Sage, Thousand Oaks, CA, pp. 86-105.

Livingstone, S, Haddon, L, Görzig, A & Ólafsson, K 2010, 'Risks and safety for children on the internet: The UK report: Full findings from the EU kids online survey of UK 9-16 year olds and their parents', EU Kids Online, London.

Livingstone, S, Haddon, L, Görzig, A & Ólafsson, K 2011, 'Risks and safety on the internet: The perspective of European children: Full findings and policy implications from the EU kids online survey of 9-16 year olds and their parents in 25 countries', EU Kids Online, London.

Loeber, R, Farrington, D & Petechuk, D 2003, *Child delinquency: Early intervention and prevention*, U.S. Office of Juvenile Justice and Delinquency Prevention Washington, DC.

McCord, J 2003, 'Cures that harm: Unanticipated outcomes of crime prevention programs', *The ANNALS of the American Academy of Political and Social Science*, vol. 587, no. 1, pp. 16–30.

Moffitt, T 2018, 'Male antisocial behaviour in adolescence and beyond', *Nature Human Behaviour*, vol. 2, no. 3, pp. 177-186.

Moffitt, T, Caspi, A, Dickson, N, Silva, P & Stanton, W 1996, 'Childhood-onset versus adolescent-onset antisocial conduct problems in males: Natural history from ages 3 to 18 years', *Development and Psychopathology*, vol. 8, no. 2, pp. 399-424.

Moore, T & Clayton, R 2011, 'Ethical dilemmas in take-down research', In G Dietrich and K Sako (eds) Financial Cryptography and Data Security, (lecture notes in *Computer Science*, vol. 7126, pp. 154–168), Springer: Berlin, Germany.

Murray, J & Farrington, D 2010, 'Risk factors for conduct disorder and delinquency: Key findings from longitudinal studies', *The Canadian Journal of Psychiatry*, vol. 55, pp. 633–642.

Nansen, B, Chakraborty, K, Gibbs, L, MacDougall, C & Vetere, F 2012, 'Children and digital wellbeing in Australia: Online regulation, conduct and competence', *Journal of Children and Media,* vol. 6, no. 2, pp. 237–54.

Prenoveau, J, Craske, M, Zinbarg, R, Mineka, S, Rose, R & Griffith, J 2011, 'Are anxiety and depression just as stable as personality during late adolescence? Results from a three-year longitudinal latent variable study', *Journal of Abnormal Psychology*, vol. 120, no. 4, pp. 832.

Scott, L, Crow, W & Erickson, R 1985, *Robbery as robbers see it*, Southland Corporation: Dallas, TX.

Sherman, L 1993. 'Defiance, deterrence, and irrelevance: A theory of the criminal sanction', *Journal of Research in Crime and Delinquency*, vol. 30, no. 4, pp. 445-473.

Shaw, I, Greene, J & Mark, M 2006, *The Sage handbook of evaluation* (eds), Sage: London, UK.

Shin, W & Lwin, M 2016, 'How does 'talking about the internet with others' affect teenagers' experience of online risks? The role of active mediation by parents, peers, and school teachers', *New Media & Society*, vol. 19, no. 7, pp. 1109-1126.

Sloan-Howitt, M & Kelling, G 1990, 'Subway graffiti in New York City: 'Getting up' vs. meaning' it and 'cleaning' it', *Security Journal,* vol. 1, no. 3, pp. 131–136.

Soska, K & Christin, N 2015, 'Measuring the longitudinal evolution of the online anonymous marketplace ecosystem', in Proceedings of the 24th USENIX Security Symposium, Washington, D.C., pp. 33–48.

Storvoll, E & Wichstrøm, L 2003, 'Gender differences in changes in and stability of conduct problems from early adolescence to early adulthood', *Journal of Adolescence*, vol. 26, no. 4, pp. 413-429.

Welsh, B & Farrington, D 2001, 'Toward an evidence-based approach to preventing crime', *The ANNALS of the American Academy of Political and Social Science,* vol. 578, no. 1, pp. 158–173.

Williams, M 2006, *Virtually criminal: Crime, deviance and regulation online*, Routledge.

Yar, M 2005, 'Computer hacking: Just another case of juvenile delinquency?', *The Howard Journal,* vol. 44, no. 4, pp. 387–99.