N0770489

Dr Daria Kuss

August 2019

Exploring the narrative on Internet Addiction and cybercrime. A systematic literature review.

Alex Paradise

MSc Cyberpsychology

Psychology Division
School of Social Sciences
Nottingham Trent University

Abstract

Cybercrime has been highlighted as a significant threat to national security in the UK. Therefore, the prevention of online offending is topic of governmental interest. A growing body of research focuses on behavioural addictions and their influence on online behaviour. Research into this condition has the potential to have significant influence on criminal justice policy. This systematic literature review focuses on the concept of 'Internet Addiction' (IA) and the current narrative linking the condition to online crime. The empirical basis of these claims is examined.

Research suggests that IA may be linked to online sexual and domestic abuse, harassment, digital piracy and hacking. However, the evidence base appears to be limited presently and largely consists of correlational studies. There is a lack of consistency in IA conceptualisation and measurement. Further and more robust research is required for IA literature to have the potential to impact public policy.

1. Introduction

1.1 Background

The invention of the internet has revolutionised modern society. Described as the 'Digital Revolution' and 'age of technology' (Collins & Halverson, 2018) the turn of the century has seen unprecedented technological development and innovation. While the Digital Revolution has had may positives there may also be downsides. Researchers have argued that one of these may be the emergence of a new clinical disorder, Internet Addiction (IA) (Christakis, 2010).

This literature review aims to explore the contemporary narrative on the relationship between IA and cybercrime; and to what extent this is evidence based. Although research has touched upon IA, most notably by an Interpol endorsed paper (Aiken, Davidson & Amann, 2016) the role IA may play in online crime is not yet fully understood. Cybercrime is seen as having great significance on an international scale (HM Government, 2010). Understanding the drives and motivations of those engaging in online criminality is needed to inform effective public policy. The nature of the relationship between IA and cybercrime, if one can be established to exist, may be relevant to this aim. Research has claimed individuals with an IA are associated with engaging in, or being the victims of, cybercrime (Navarro, Marcum, Higgins & Ricketts, 2014; Haddlington, 2017; Kostyunina, Latypova & Sirazeeva, 2018). However, correlation is not causation and causation of IA as a factor in increased online offending would need to be established.

Researchers have begun to explore the influences leading to young people becoming engaged in cybercrime (Aiken, Davidson & Amann, 2016). Some academics have claimed that the current policing strategies focusing on reducing youth cybercrime are counter-productive (Holt, Brewer, Goldsmith, 2018). It has been suggested that those engaged in reducing youth cyber offending should explore the dynamics of internet use and the background of those involved (Holt, Brewer, Goldsmith, 2018). Frameworks of behavioural addiction are a potential explanation of the escalation of online offending and challenges in preventing recidivism (Nykodym, Ariss, & Kurtz, 2008). The role of IA in escalating online criminality and victimisation remains under-researched (Aiken, Davidson & Amann, 2016) and presently it is not fully understood why an IA may result in criminal/deviant behaviours (Levi, Button & Whitty, 2017).

Researchers have called for greater awareness of IA among public policy makers (Tomažič, & Bessa-Vilela, 2017). Within the UK the treatment of substance addictions is a long established and integrated part of the criminal justice system (Barton, 1999). Should the evidence justify investment, it is not inconceivable that the future of cybercrime prevention will also involve treatment programs for behavioural addictions.

1.2 Internet Addiction

Internet Addiction is conceptualised as a behavioural addiction characterised by excessive use of internet-based applications, causing harm or severe disruption to the sufferer's lifestyle (Kuss, Griffths, Karila & Billieux, 2014). Shaw and Black (2008) highlighted that IA is typically described as causing impulsive behaviours or poorly controlled preoccupations online. These behaviours lead to the impairment in daily life and emotional distress. IA has received increasing interest among international researchers and the media (Shaw and Black, 2008).

The *Diagnostic and Statistical Manual of Mental Disorders* (DSM-V) (American Psychiatric Association, 2013), called for further research into what it termed ‘Internet Gaming Disorder’ (IGD). This disorder is related to but conceptually distinct from IA, as IGD limits itself to the arena of computer gaming (Kuss, Griffiths, & Pontes, 2017). Consideration of IGD follows an international trend of interest in behavioural addictions (Aarseth et al., 2017). Calls for further research into IGD rather than IA has received criticism that the DSM is conceptually confused (Kuss, Griffiths, & Pontes, 2017) and artificially narrow in its focus.

Critics argue that the term 'Internet addiction' is misleading (Starcevic, 2013; Starcevic & Aboujaoude, 2017; Ryding & Kaye, 2018). Starcevic (2013) argued that it was not the technology of the internet, but online content that could be addictive. Indeed, it has been suggested some forms of internet use may be more addictive than others (Kuss, Van Rooij, Shorter, Griffiths, & van de Mheen, 2013), which could support the argument that IA research should focus on specific forms of content. Ryding and Kaye (2018) suggested that the narrative around IA may be explained by the concept of moral panics (Cohen, 2011). Ryding and Kaye (2018) argue that most forms of new media are affected by a luddite media narrative which assumes new technology is harmful. However, a systematic review of neuro-imaging studies into IA (Kuss & Griffths, 2012b) highlighted similarities between the brains of substance addicts and those suffering with IA. This study suggests that neurotransmitters, neural circuitry and behaviour is altered in IA in a similar way to substance addictions. It could be argued that while different internet mediums, and different drugs, are available the overarching label of 'addict' is still appropriate.

IA can be expressed by dysfunctional behaviour in numerous online contexts, including online gaming, gambling, shopping and use of social media (Kuss, Griffiths, Karila & Billieux, 2014). Griffiths (2005) argued that several factors were common to behavioural addictions and substance addiction; salience, mood modification, tolerance, withdrawal, conflict and relapse. Evidence suggests that behavioural addictions may also show similar neurological markers to substance addictions (Potenza, 2014). Reported prevalence rates of IA in the population have varied between 0.8% to 18.3% in different studies (Kuss & Griffiths, 2015). This variation may be a product of samples in these studies being drawn from different demographics and nationalities (Kuss & Griffiths, 2015). A common criticism of IA research is inconsistency in assessment instruments between studies (Kuss & Griffiths, 2015; Mueller, et al, 2017).

It has been proposed that IA may have real world consequences. Researchers have already proposed that employees suffering from an IA represent a cyber-security vulnerability for businesses (Hadlington, 2017; Hadlington & Parsons, 2017). Research has shown that reduced impulse control and behavioural inhibition is a product of an IA (Dong, Lu, Zhou, & Zhao, 2010), which may partially explain why an IA is a potential vulnerability in the work place. It has also been suggested that Problematic Mobile Phone Use (PMPU), may represent a related behavioural addiction (Billieux, Maurage, Lopez-Fernandez, Kuss, & Griffiths, 2015). Furthermore, it is possible that PMPU is a symptom of IA. PMPU has been linked to increased risk of cyberbullying and users engaging in dangerous patterns of use, such as driving whilst using a phone (Billieux et al., 2015).

There is an established link between substance addiction and crime (Morse, 2017). Given evidence of similarities between substance and behavioural addiction, it is possible that there is a parallel relationship exists between IA and crime. There may be value in police and policy makers having an awareness of IA. However, there is a great deal of debate on the nature of the condition.

1.3 Cybercrime

In 2010 the UK government declared cyber-attacks by criminals and foreign state actors a Tier 1 threat to national security (HM Government, 2010), putting the identified risk at the same level as terrorism or armed conflict. The British government defines cybercrime as an illegal act which is only possible use of Information and Communications Technology, or, a traditional crime utilising computers, computer networks or other forms of ICT in the commission of the offence (HM Government, 2016). Similarly, to research surrounding IA it has been argued that the response to cybercrime by the public and authorities shows signs of a moral panic (Wall, 2008). However, estimates show that cybercrime is costing the global economy approximately $1 trillion per year (HM Government, 2010). Given the significant financial impact of cybercrime it is difficult to dismiss this offending as a moral panic.

This literature review utilises Aiken, Davidson and Amann's (2016) whitepaper as a source for search terms. Aiken, Davidson and Amann's (2016) report was supported by Europol's European Cybercrime Centre, Interpol and the National Crime Agency. Under their conceptualisation, cybercrime is divided into two sub categories:

1) Computer Crimes,
Also described as "True" cybercrimes, these include illegal acts which target computer systems or networks and are purely committed online.

2) Computer related crime,
The use of computers to facilitate types of crime also seen offline.

This conceptualisation is therefore well aligned to the definition of cybercrime being utilised in the UK government. Within Aiken, Davidson and Amann's (2016) report several forms of cyber-criminality were identified and summarised as shown in Table 1. While this list was non-exhaustive it covered key cybercrimes thought to represent current threat.

Computer Crimes	**Computer Related Crimes**
Hacking (overarching crime type)	Computer related forgery
Illegal access	Computer related fraud
Illegal interception	Child Sexual Exploitation
Data interference	Child Sexual Abuse Material
System interference	Computer assisted copyright infringement
Malware writing	
Botnet operation	
Website defacement	
Ransomware attack	
Distributed Denial of Service	

Table 1. Cybercrime terms Aiken, Davidson & Amann (2016)

1.4 Research Questions

(i) What is the narrative on the relationship between cybercrime and IA in the current academic literature?
(ii) To what extent is this narrative based on empirical research?
(iii) Where may knowledge gaps exist in this topic?

2. Method

2.1 Design, Materials and Analyses

This study conducts a systematic literature review of previous peer-reviewed papers on the topic of IA and Cybercrime. The literature search utilised Web of Knowledge, conducting a review across all database held on this online website. The Web of Knowledge database was selected due to its broad collection of literature published across several fields, allowing multidisciplinary content to be included. The search period was limited to the last decade (2009-2019) to ensure that the literature review focused on current papers. Results were set to be limited to studies published in an English language format. The search process was broken down into a series of searches, which was intended to assist in identifying possible literature gaps.

2.2 Identifying Papers and Inclusion Criteria

Papers were identified through keyword searches;

(1) Initially two separate searches on ‘Internet Addiction’ and ‘Cybercrime’ (and derivatives) was conducted returning over three thousand and two thousand results respectively. Using the combine function, only fourteen studies appeared in both sets, representing 0.4% of IA literature. Results were combined to gain an indication of what proportion of IA research explored cybercrime.

(2) Secondary individual searches were conducted on the topic of ‘Internet Addiction’ and a search term derived from Aiken, Davidson and Amann’s (2016) summary of cybercrime types. Individual searches were conducted to identify the number of papers associated with each particular topic, terms used are shown in Table 2. The majority of searches found no results, however searches on Internet Addiction and; Hacking (and derivatives), Malware, Fraud, Child Sexual Exploitation and Sex Offender collectively returned twenty-one results. Five papers had been identified in multiple searches. In total thirty studies were assessed against the inclusion criteria.

Search terms	
Hack*	Distributed Denial of Service
“System Interference”	Fraud
“Illegal Interception”	Forgery
“Illegal Access”	CSE
"Data interference"	Child Sexual Exploitation
Malware	CSAM
Botnet	Child Sexual Abuse Material
"Website defacement"	IIOC
Ransomware	Indecent Images of Children
DDoS	Sex Offender
	Copywrite

Table 2. Search terms derived from Aiken, Davidson and Amann’s (2016) paper.

Inclusion criteria for the studies were that the paper: (i) has a full text version of the paper available in an English language format, (ii) published in a peer reviewed conference paper or journal, (iii) the paper explores or claims a relationship between IA and Cybercrime.

3. Results and Discussion

3.1 Excluded studies

Seventeen of the identified studies were excluded from the literature review. The most common reason for this was the researcher being unable to identify an English language version of the paper. The majority of studies excluded were Korean language papers, which provided an English version of the abstract but not a full text (Jeong, 2009; Jun, 2015; Jun, 2016; Kim, 2012; Kim, 2013; Kim, 2018; Kim & Kang, 2010; Kim & Seo, 2012; Lee, 2013; Lee, 2009; Lee, & Song, 2017; Park, 2012; Shin, 2011, Wan, 2009). Whiles these papers were detected as being in English erroneously by Web of Science, the abstracts do suggest a strong narrative on the relationship between IA and Cybercrime exists in in the Korean literature.

The abstracts of some of these studies suggest that they may directly explore the relationship between IA and Cybercrime or online victimisation (Kim, 2013; Kim & Seo, 2012; Lee, 2009; Lee, & Song, 2017; Jeong, 2009, Kim & Kang, 2010). It was noted that two studies appeared to suggest the internet caused wide array of social ills, (Lee & Song, 2017; Jeong, 2009) which was echoed to an extent in the other abstracts. This may indicate signs of moral panic (Cohen, 2011) within the Korean literature. The remaining Korean language papers appeared to link IA and Cybercrime in their abstracts, but not study both concepts. The abstracts appear to show IA being considered to be a cause, or commonly found alongside, deviant online behaviour. Despite this, without access to translated versions of the papers it is challenging to fully comment on the narrative of current Korean literature. It may be of value for future researchers to translate and review the findings of these papers. A further paper was excluded as only a Russian language version of the paper could be identified (Lazhintseva & Bochaver, 2015). Two papers on IA were erroneously linked to cybercrime (Brewer, 2019; Öze, 2018).

3.2 Selected papers

Researchers from across the globe have contributed to the narrative regarding IA and Cybercrime. The included papers contributions from the United States, United Kingdom, Australia, Spain, Russia, Slovakia, Turkey, South Korea and Taiwan. A broad geographical spread suggests that IA's influence on deviant online behaviour is a matter of international interest. The selected papers are displayed in Table 3.

Study (Year)	**Title**	**Author(s)**	**Research Field(s)**
2011	An adolescent case with Internet Addiction and hacking: how are we dealing with this diverse spectrum of disorder?	Solmaz, & Saygili	Psychiatry
2013	"Internet sexual offending: Overview of potential contributing factors and intervention strategies"	Neto, Eyland, Ware, Galouzis & Kevin	Forensic Psychology
2014	"Addicted to pillaging in cyberspace: Investigating the role of internet addiction in digital piracy"	Navarro, Marcum, Higgins & Ricketts	Human Computer Interaction
2015	"Internet Addiction Factors"	Tikhonova & Bogoslovskii	Human Computer Interaction / Psychology

2016	“Internet misconduct impact adolescent mental health in Taiwan: The moderating roles of internet addiction”	Yu, & Chao	Human computer interaction/ Psychology
2017	“Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours.”	Haddlington	Psychology
2017	“An analysis work on correlation of internet addiction and school age groups.”	Jun	Psychiatry/ Psychology
2017	“Ongoing criminal activities in cyberspace: From the protection of minors to the Deep Web.”	Tomažič, & Bessa-Vilela	Criminology
2018	“Prevention of Students’ Victim Behavior on the Internet”	Kostyunina, Latypova & Sirazeeva	Psychology Education studies
2018	“Explaining cyber deviance among school-aged youth.”	Lee	Psychology
2018	“Ethical considerations for mental health clinicians working with adolescents in the digital age.”	Sussman & DeJong	Psychiatry/ Clinical Psychology
2019	“Smartphone addiction: psychosocial correlates, risky attitudes, and smartphone harm.”	Herrero, Urueña, Torres, & Hidalgo	Psychology
2019	Online Pursuit in the Twilight Zone: Cyberstalking Perpetration by College Students	Reyns	Criminology / Victimology

Table 3. Included papers

3.3 Research designs and measures

Thirteen papers were found to satisfy the criteria for inclusion. Eight studies utilised self-report surveys to explore correlational relationships. Various psychometric tests were utilised by these papers. One paper (Solmaz, & Saygili, 2011) was a case study of a young hacker being treated for IA. Six out of these nine studies focused on young participants, with the remaining three having samples from a broader pool of participants.

Four papers were categorised as literature reviews, none of which, primarily, explored a link between IA and any form of cybercrime. Two of these papers discussed IA in a medical context (Tikhonova & Bogoslovskii, 2015; Sussman & DeJong, 2018) whilst the remaining papers considered factors which may contribute to online sex offending and children's vulnerability online respectively (Neto, Eyland, Ware, Glaouzis & Kevin, 2013; Tomažič, & Bessa-Vilela, 2017). The populations researched are shown in Table 4.

Tomažič, and Bessa-Vilela's (2017) paper, whilst primarily a review of literature, also statistically analyses cybercrime data from the Slovenian police; exploring crime trends between 2011 and 2015.

Study	Research population	Demographic information
Solmaz, & Saygili, (2011)	Case study of a young Turkish hacker suffering from IA.	A 16-year-old Turkish male, first year high school student.
Navarro, Marcum, Higgins & Ricketts (2014)	1617 American students	Participants aged 14-18 years (average 15.77) 49% male. 72% white.
Yu & Chao, (2016)	8480 Taiwanese students	Participants aged 13-18 years (mean 16.45, SD 0.93).
Haddlington (2017)	538 UK based participants in full or part time employment	Participants aged 18 – 84 years. 55% female.
Jun (2017)	Between 16,000 – 24,000 South Korean students.	Participants drawn from South Korean education system (Kindergarten to University), with between 4,000 -6,000 sampled each year between 2010 - 2014
Kostyunina, Latypova & Sirazeeva (2018)	127 Russian university students	Participants aged between 18-21 years, drawn from the student body of a Russian psychology department.
Lee (2018)	779 South Korean students	Participants aged between 10 and 16 years. 50.77% male.
Herrero, Urueña, Torres, & Hidalgo (2019)	526 Spanish smartphone using Spanish residents.	Participants drawn from the ‘’Cybersecurity and Confidence in Spanish Households national survey’ (2015). 51.9% male. Population screened to be representative of total Spanish population.
Reyns (2019)	759 American students	Participants had an average age of 20 years. 61% female. 87% white. Drawn from the student body of a large US midwestern university.

Table 4. Research populations

Multiple measures of IA or associated symptoms were utilised by the various studies. Solmaz and Saygili’s (2011) case study does not state how IA was diagnosed, however the paper does cite Canan, Ataoglu, Nichols, Yildirim and Ozturk (2010) who tested an IA psychometric with a Turkish research population. It could be speculated that this was the diagnostic tool used, however it is difficult to state with certainty.

Psychometrics used in the literature to assess IA or associated symptoms included; 'Internet Related Problem Scale' (Armstrong, Phillips & Saling, 2000), 'Abbreviated Impulsiveness Scale' (Coutlee, Politzer, Hoyle, & Huettel, 2014), 'Online cognition scale' (Davis, Flett & Besser, 2002), 'Cyber-Communication Addiction Scale' (Toncheva, 2012), 'Five dimensions of self-control scale' (Grasmick et al., 1993), 'Cyberstalking Perpetration scale' (Reyns, 2019) and an unnamed scale created by Yu & Chao (2016). Data from two governmental surveys was also used as a measure of IA or its purported symptoms; including data from the 'Cybersecurity and Confidence in Spanish Households national survey' (cited in Herrero, Urueña, Torres, & Hidalgo, 2019) and a measure produced by the Korea Information Society Agency (cited in Jun, 2017).

No two papers utilised the same method of measuring IA or symptoms associated with the condition. This represents a weakness in the literature as it cannot be assumed that the measures consistently tested IA between studies. As no standardised conceptualisation of IA is adopted it is possible that variation exists in what these instruments measure. The researchers did not generally consider the validity of the measure used in their study vs that used by other IA researchers. As such the similarity or differences between the measures is unknown. This criticism has previously been levelled at IA research, generally (Kuss & Griffiths, 2015).

3.4.1 Self-Control, impulsiveness and emotional regulation

The literature consistently and unanimously linked IA to negative social, emotional or physical issues for individuals with IA. A recurring theme was a proposed link between low self-control and both online offending and online victimisation. The narrative appears to broadly suggest that IA is a cause or contributing factor to some forms of cybercrime.

The earliest paper identified (Solmaz, & Saygili, 2011), a Turkish case study, discussed the treatment of a 16 year old male who had developed IA after joining an online hacking community. This individual was found to suffer from withdrawal symptoms when prevented from accessing the internet. These symptoms included anger and crippling anxiety. The male was described as spending up to twenty hours a day online, causing significant detriment to his ability to maintain offline social relationships and having a negative effect on his previously good grades at school. The individual felt a constant need to be available for communication with other hackers in his group.

Similarly to Solmaz and Saygili's (2011) findings, Kostyunina, Latypova and Sirazeeva (2018) found Russian students scoring highly on the Cyber-Communication Addiction scale to engage in anti-social behaviour, display impulsive emotional reactions, show impatience, anger and carelessness and have difficulty in making judgements. Impulsive behaviour, low self-control or difficulties regulating emotions were associated with IA by the majority of the papers. IA was suggested as a direct cause of dysfunctional and or criminal online behaviour by several papers (Solmaz, & Saygili 2011, Haddlington, 2017; Jun, 2017; Kostyunina, Latypova & Sirazeeva 2018; Lee, 2018; Herrero, Urueña, Torres, & Hidalgo 2019). Other papers linked impulsive behaviour and low self-control to cyber offending, and discussed IA as being a possible cause (Neto et al., 2013; Navarro, Marcum, Higgins & Ricketts 2014; Rayns, 2019). Low self-control appeared to be the primary link between IA and cybercrime in the overarching narrative.

Several studies linked IA with particular crime types. Neto et al. (2013) highlighted a link between low self-control and online sexual offending. Similarly, Reyns (2019) reported a correlation between low self-control and engaging in cyberstalking/online pursuit behaviours. Lee (2018) found a connexion between low-control and engagement in online harassment, whilst IA was associated in the literature with cyberbullying (Yu & Chao, 2016). Within the current narrative, IA is suggested to be an emerging factor in abusive online behaviour. This may be relevant to sexual and domestic abuse offending, as well as general harassment behaviours.

There are also indications of computer-dependent offending being linked to the condition. Navarro, Marcum, Higgins and Ricketts's (2014) findings suggest those displaying IA symptoms are more likely to engage in software piracy, while Lee (2018) found a correlation between the condition and engaging in computer hacking. However, some caution should be exercised in claiming a directionality of this relationship. In Solmaz, and Saygili's (2011) case study it is difficult to establish whether IA resulted in the individual becoming involved in hacking, or that a heavy engagement with a hacking focused peer group later resulted in the prevalence of a mental health condition.

IA was claimed to be a "Global major mental health issue" by Yu and Chao (2016). Several papers propose a link between IA, depressive illness (Jun, 2017, Lee, 2018) and social anxiety (Solmaz & Saygili, 2011; Lee, 2018; Herrero, Urueña, Torres, & Hidalgo, 2019). Higher levels of the personality trait neuroticism were also associated with developing an IA (Herrero, Urueña, Torres, & Hidalgo, 2019). Whilst several studies proposed a comorbidity between IA and disorders involving low mood, the directionality of this relationship was not empirically scrutinised. Tikhonova and Bogoslovskii (2015) cite a Russian study (Lisetskii & Lityagina, 2016) which found that 75% of those struggling with an IA also had issues with alcohol or drugs.

3..4.2 Influence of peer networks

Within the literature there are several indications that peer networks may be significant to providing evidence for the existence of a relationship between IA and cybercrime. In Navarro, Marcum, Higgins and Rickett's (2014) study IA was positively correlated with engaging in software piracy. However, the study included three forms of piracy; software, music and film. Association with pirating peers was also correlated with all three forms of piracy studied. It is suggested that Social Learning Theory (SLT) (Bandura & Walters, 1977) may explain young people's likelihood of engaging in digital piracy (Navarro, Marcum, Higgins and Rickett, 2014). This suggestion is consistent with the findings of other research on social learning and digital piracy (Hinduja & Ingram, 2009; Morris, & Higgins, 2010). Navarro, Marcum, Higgins and Rickett (2014) suggest that peers observing, and imitating others combined with IA symptoms may fully account for the likelihood of engaging in software piracy. This may suggest that IA is a lesser, but significant, factor in understanding why intellectual property theft occurs.

Herrero, Urueña, Torres, & Hidalgo (2019) found that those with low levels of social support were more likely to engage in addictive behaviour with smartphones. Research has suggested that some online behaviours are more common among IA suffers. Engagement in online gaming and social networking are particularly prevalent among those showing IA symptoms (Kuss, Griffiths, & Binder, 2013; Kuss, van Rooij, Shorter, Griffiths, & van de Mheen, 2013). This may be the product of disproportionately young research populations. However, explanation could be that peer networks are significant in the development of an IA and the condition's interaction with criminogenic environments. The interaction between the natural impulsiveness of young people, the impact of behavioural addictions and membership of deviant peer groups may be key drivers in cybercrime offending (Aiken, Davidson & Amann, 2016).

3.4.3 Treatment and prevention

As noted previously, it is plausible that treatment for behavioural addictions may form part of public policy on cybercrime prevention in the future. While IA may influence online offending, this information is less useful without a method of reducing IA's impact. Within the literature, two research papers discuss treatments for an IA: Solmaz and Saygili (2011) and Kostyunina, Latypova and Sirazeeva (2018).

Solmaz and Saygili (2011) cite that the 16 year old male in their case study received Cognitive Behavioural Therapy (CBT) and pharmacological support, in conjunction with an intense period of therapy; every other day for two weeks, followed by a weekly session for six weeks. Therapy focused on strategies aimed at better emotional self-regulation. Pharmacological treatment using sertraline, carbamazepine and risperidone was deployed alongside this therapy. The efficacy of the treatment was evaluated by the authors as successful by helping the individual to reengage with real world social groups/activities, coming away from heavy engagement with the hacking community. Within the paper it is not explained what measures were used to diagnose an IA in the participant. Similarly, the detail of how the treatment was evaluated as successful is limited. A high probability of relapse is an established factor in behavioural addictions (Griffiths, 2005; Koob & Volkow, 2016). It is unknown how long after treatment the evaluation of outcomes took place.

Kostyunina, Latypova and Sirazeeva's (2018) main aim was to evaluate a cybercrime prevention program being run at Kazan Federal University. The intervention program aimed to achieve what is described in the UK as ‘target hardening’. This was to be accomplished by encouraging students not to engage in behaviours that were likely to result in becoming victim to harassment, fraud or other online crime. This multidisciplinary program involved teaching inputs from specialists in Sociology, Psychotherapy, Medicine, Psychology and Education. Utilising traditional teaching inputs, including those from specialists, seminars, modern education methods utilising digital technology and one to one counselling.

This program had three major components;

1) A cognitive training program which appeared to teach Cyberpsychological principles and increase understanding of the impact of the online environment on behaviour and cognition.

2) A focus on the individual psychological make up of the student and their particular strengths and vulnerabilities in relation to online victimisation.

3) Activity based training, mainly relating to more social inputs encouraging interaction with students and educators. This section included psychological counselling.

Utilising psychometric testing and surveys, the efficacy of the prevention program was evaluated by the authors, who cited a decrease in the proportion of the sample engaging in high risk online behaviour from 13.3% to 6.2%. The study’s measure of IA (‘Cyber-communication addiction’) found that the proportion of the group identified as having high levels of IA reduced from 19.6% to 9.4%. Kostyunina, Latypova and Sirazeeva (2018) concluded that behavioural addictions can result in online victimisation, but it is possible to reduce this risk through preventative interventions. In their program, counselling combined with critical thinking skills training and lessons on the nature of online risk and control strategies for impulsive behaviour was provided. This was deemed to be effective in reducing victimisation risk. This research suggests that therapy and prevention programs may be effective in reducing both cyber offending and victimisation. However, this study had a relatively small sample of 127 participants. With no further studies cited utilising their prevention methodology, claims of generalisability may not be justified.

The discussion of treatment in these papers is consistent with other researcher's comments. Pontes, Kuss, & Griffiths (2015) highlight that a growing body of evidence suggests neurological similarities exist between substance and internet addictions. This similarity is significant as models of treatments used for individuals with substance addictions may be effective in treating IA. It is noted that such treatments, including pharmaceuticals and CBT, are already being used to treat IA (Pontes, Kuss, & Griffiths, 2015; Santos et al., 2016). However, the evidence base for pharmaceutical treatment remains limited due to a lack of research (Pontes, Kuss, & Griffiths, 2015).

3.4.4 Evidential basis of the narrative

There are strengths to the identified experimental evidence base for a relationship between IA and Cybercrime. The negative influence of IA and how this may influence offending and victimisation is highly consistent. Research populations were located in numerous countries and different cultures, which may suggest a consistent global relevance. The sizes of the populations studied varied, with some very large (Navarro, Marcum, Higgins & Ricketts, 2014; Yu & Chao, 2016; Jun, 2017). The size of these samples increases the reliability of the results. The evidence base within these studies points to low self-control, impulsive behaviour and deficits of emotional regulation as the specific aspects of IA which may cause criminal behaviour.

However, there are also several weaknesses. Pontes, Kuss and Griffiths (2015) identified that research into the treatment of IA suffered from empirical limitations. Similar to their findings, the present literature review identified inconsistent measures of IA utilised across the studies. The studies largely reported correlational relationships, which limit the ability to claim causality. Future research would benefit from utilising control or comparison groups and randomisation of the conditions. Additionally, in several studies, limited information was available about the demographics and characteristics of the participant groups studied. Furthermore, the process by which IA or dysfunctional impulsive behaviour was measured was not always clear.

The generalisability of the research on this topic could be improved by the adoption of a standardised concept of IA as a condition. Similarly, a standardised and validated measure would improve the generalisability of findings. Key to this research area is the concept that IA may drive impulsive behaviour, resulting in various forms of criminality. Therefore, research is required to more strongly establish the evidential basis for this purported link.

A promising area of IA research is establishing neurological patterns among IA suffers and similarities with substance addicts (Potenza, 2014; Kuss & Griffths, 2012b; Pontes, Kuss, & Griffiths, 2015). The present research largely utilises self-report measures to establish levels of criminal or deviant behaviour. There, an opportunity exists to directly study cybercrime offender populations within the criminal justice system. This may allow greater certainty of the online behaviours of participants and offer a greater insight into the prevalence of IA among this group.

Furthermore, it is notable that the majority of the papers identified focused on young people. It is uncertain if the received wisdom that cybercrime relates primarily to the young is still valid. Rashid, et al,

(2013) highlights that cybercrime is committed by individuals from all age groups. There may be value in understanding how IA may affect the online behaviour of other age groups.

3.4.5 Limitations

The present study utilised the search function of Web of Knowledge, an online scientific citation indexing service. Web of Knowledge allows access to multiple databases and as of 2019 10,943 individual documents (Airyalat, Malkawi & Momani, 2019). While the scope of the site is broad, less than half of the journals listed in Ulrich's Periodicals Dictionary are present (Mongeon & Paul-Hus, 2016). Whilst the search it conducts is expansive it cannot be claimed that Web of Science will contain papers from every journal in a given discipline (Airyalat, Malkawi & Momani, 2018). Additionally, the site primarily focuses on English language journals; meaning that journals from countries with other primary languages may be underrepresented (Mongeon & Paul-Hus, 2016). As such it cannot be claimed that a literature review conducted using the site, however rigorous, will identify all papers on a given topic. It is also a limitation of the researcher that only papers published in the English language could be reviewed. Given the international interest in IA and cybercrime it is possible that many studies have not been translated into English. Translation of such papers could unlock new insights into IA and progress understanding of the condition.

A second criticism made of Web of Knowledge and similar databases is that the site is vulnerable to manipulation (Gasparyan, 2015). It is possible for authors, through methods such as heavy self-citation, to rank more highly on the site and become more visible (Gasparyan, 2015). This is not perceived to be a weakness of the present review as all search results were screened for inclusion rather than just the most prominent.

As previously discussed, variations exist in the literature in the conceptualisation and measurement of IA. Furthermore, it is evident that variability exists within the term used to describe the condition (Yu & Chao, 2016; Haddlington, 2017; Reyns, 2019). The international nature of the literature may also result in differing translations of key terms, which may have resulted in literature being overlooked. This challenge may also impact non-English speaking researchers, with translation of English studies into other languages being limited. Both Russian papers highlighted very little IA research is being published in Russian (Tikhonova & Bogoslovskii, 2017; Kostyunina, Latypova & Sirazeeva, 2018).

Two Web of Knowledge searches for 'Internet Addiction' and 'Cybercrime' and then combined to find common results. The purpose of this was to gain an understanding of the rough proportion of IA research also considering cybercrime, which appeared to be a fraction of a percent (0.4%). Given the limitations of the methodology, and the further papers identified, this figure may be overly conservative. However, the search does suggest IA's relation to cybercrime is a minority research topic within the field. The current evidence base, while small, justifies further research due to the global significance of cybercrime.

The additional searches based on Aiken, Davidson and Amann's (2016) summary of cybercrime types identified further papers which were included in the final review. Aiken, Davidson and Amann (2016) state that this is not a comprehensive list of all cybercrime types, but current key forms of online offending are included. Therefore, it is possible that some studies fell outside of this typology and were not identified.

Additionally, it could be questioned if Aiken, Davidson and Amann's (2016) division between 'computer enabled' and 'computer dependent' cybercrime is necessary. In Tikhonova and Bogoslovskii's (2015) paper, it is suggested that those suffering from IA may also have an increased likelihood of drug and alcohol abuse. It could be argued that the division of cybercrime from traditional offending is artificial and there may be common driving factors. Furthermore, it is possible that IA is an influence of offline crime, such as traffic offences (Billieux, et al, 2015). If this is the case, it could be questioned whether distinguishing older crime types now utilising a computer from crimes dependent computers is meaningful. Further research would be important in exploring the validity of this division.

4. Conclusion

This systematic review explored the current academic narrative on the relationship between Internet Addiction and cybercrime. The evidence suggests that limited research has been conducted on this topic, with only thirteen papers identified as contributing to the narrative. The identified literature suggests that there is a link between a symptom of IA, low self-control/impulsive behaviour and cybercrime. Indications of specific links to abusive online behaviour, copywrite theft and hacking were found. IA is suggested to be comorbid with mental health problems characterised by low mood and issues with emotional regulation. There are also some indications IA may be linked to offline offending, such as illegal substance use (Tikhonova & Bogoslovskii, 2015).

However, the empirical basis of these claims could be challenged. The majority of research studies identified a correlational relationship between IA/low self-control and cybercrime. This research provides a weak basis for a claim that IA may be a cause of online offending. Therefore, further research is required before a causal relationship can be established with empirical confidence. Additionally, it is also necessary to establish a causal relationship between IA and diminished levels of self-control. It could be questioned whether the amount of research focusing on young people is proportionate to the internet using population. One of the significant challenges of the current research base is a lack of consistency in IA conceptualisation and measurement (Kuss & Griffiths, 2015). A more consistent approach to measuring IA levels would improve generalisability of findings.

Several gaps in knowledge exist within the current literature. IA may influence online offending/victimisation in older age groups, however the majority of research was conducted on young people within the education system. Direct research of identified cyber offenders and victims may advance the evidence base, giving more confidence in online behaviours than self-report surveys. A potential link between IA and online sex offending is suggested (Neto, Eyland, Ware, Galouzis & Kevin, 2013) and would benefit from further focus. Similarly, research has indicated a link between IA and online stalking (Reyns, 2019). This research area has potential implications for domestic abuse prevention, therefore further research is required. A relationship is suggested between IA, online piracy and hacking. Peer networks and social support appear to be significant in both IA development and engagement with these cybercrimes. Furthermore, a greater understanding is required of how social factors influence IA development. At this stage the understanding of the dynamics of IA's relationship with cybercrime is limited due to a lack of research.

IA research has the potential to make a significant contribution to public policy on cybercrime (Tomažič, & Bessa-Vilela, 2017). Future studies may overcome the identified issues and justify the inclusion of IA treatment programs. Therapeutic treatment of IA has the potential to become a routine part of cybercrime offender management. Neurological evidence has emerged which may underpin IA's link to impulsive behaviour. (Potenza, 2014; Kuss & Griffths, 2012b; Pontes, Kuss, & Griffiths, 2015;

Santos et al., 2016). This neurological research is an early indication that the condition may have great significance to criminal justice policy. Therefore, there is a need for further, robust research in this promising area. Support from the appropriate governmental bodies may help develop to understanding of the best ways to prevent cybercrime.

Conflict of interest

The author declares no conflict of interest. This literature review was conducted as part of an MSc in Cyberpsychology funded by the College of Policing.

References

Aarseth, E., Bean, A. M., Boonen, H., Carras, M. C., Coulson, M., Das, D., Deleuze, J., Dunkels, E., Edman, J., Ferguson, C. J., Haagsma, M. C., Bergmark, K. H., Hussain, Z., Jansz, J., Kardefelt-Winther, D., Kutner, L., Markey, P., Nielsen, R. K. L., Prause, N., Przybylski, A., Quandt, T., Schimmenti, A., Starcevic, V., Stutman, G., Van Looy, J., & van Rooij, A. (2017). Scholars' open debate paper on the World Health Organization ICD-11 Gaming Disorder proposal. *Journal of Behavioral Addictions*, 6(3), 267-270.

Airyalat, S. A., Malkawi, L. W., & Momani, S. M. (2019). Comparing bibliometric analysis using PubMed, Scopus, and Web of Science databases. *Journal of Visualized Experiments*, e58494.

Aiken, M., Davidson, J., & Amann, P. (2016). *Youth pathways into cybercrime*. London: Middlesex University. Available at: http://www.ucd.ie/geary/static/publications/Pathways_White_Paper.pdf (accessed 1st June, 2019)

American Psychiatric Association. (2013). *Diagnostic and statistical manual of mental disorders* (5th ed.). Washington, DC: Author.

Armstrong, L., Phillips, J. G., & Saling, L. L. (2000). Potential determinants of heavier Internet usage. *International journal of human-computer studies,* 53(4), 537-550.

Bandura, A., & Walters, R. H. (1977). *Social learning theory.* Englewood Cliffs, New Jersey: Prentice-hall.

Baron, N. S. (2010). *Always on: Language in an online and mobile world.* Oxford: Oxford University Press.

Barton, A. (1999). Sentenced to treatment? Criminal justice orders and the health service. *Critical Social Policy*, 19(4), 463-483.

Bian, M., & Leung, L. (2015). Linking Loneliness, Shyness, Smartphone Addiction Symptoms, and Patterns of Smartphone Use to Social Capital. *Social Science Computer Review* 33(1), 61–79.

Billieux, J., Maurage, P., Lopez-Fernandez, O., Kuss, D. J., & Griffiths, M. D. (2015). Can disordered mobile phone use be considered a behavioral addiction? An update on current evidence and a comprehensive model for future research. *Current Addiction Reports*, 2(2), 156-162.

Bondurant, S. R., Lindo, J. M., & Swensen, I. D. (2018). Substance abuse treatment centers and local crime. *Journal of Urban Economics*, 104, 124-133.

Brewer, J. (2019). Mindfulness training for addictions: has neuroscience revealed a brain hack by which awareness subverts the addictive process?. *Current opinion in psychology*, (28), 198-203.

Canan, F., Ataoglu, A., Nichols, L. A., Yildirim, T., & Ozturk O. (2010). Evaluation of psychometric properties of the Internet addiction scale in a sample of Turkish high school students. *Cyberpsychology, Behavior, and Social Networking*, 13(3), 317-320.

Cohen, S. (2011). *Folk devils and moral panics*. London: Routledge.

Coutlee, C. G., Politzer, C. S., Hoyle, R. H., & Huettel, S. A. (2014). An Abbreviated Impulsiveness Scale constructed through confirmatory factor analysis of the Barratt Impulsiveness Scale Version 11. *Archives of scientific psychology*, 2(1), 1.

Christakis, D. A. (2010). Internet addiction: a 21st century epidemic?. *BMC medicine*, 8(1), 61.

Collins, A., & Halverson, R. (2018). *Rethinking education in the age of technology: The digital revolution and schooling in America*. New York: Teachers College Press.

Davis, R. A., Flett, G. L., & Besser, A. (2002). Validation of a new scale for measuring problematic Internet use: Implications for pre-employment screening. *Cyberpsychology & behavior*, 5(4), 331-345.

Dong, G., Lu, Q., Zhou, H., & Zhao, X. (2010). Impulse inhibition in people with Internet addiction disorder: electrophysiological evidence from a Go/NoGo study. *Neuroscience letters*, 485(2), 138-142.

Gasparyan, A. Y., Yessirkepov, M., Voronov, A. A., Gerasimov, A. N., Kostyukova, E. I., & Kitas, G. D. (2015). Preserving the integrity of citations and references by all stakeholders of science communication. *Journal of Korean medical science*, 30(11), 1545-1552.

Grasmick, H. G., Tittle, C. R., Bursik Jr, R. J., & Arneklev, B. J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of research in crime and delinquency*, 30(1), 5-29.

Greenstein, S. (2015). *How the internet became commercial: Innovation, privatization, and the birth of a new network*. Princeton, New Jersey: Princeton University Press.

Griffiths, M. (2005). A ‘components’ model of addiction within a biopsychosocial framework. *Journal of Substance use*, 10(4), 191-197.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346.

Hadlington, L., & Parsons, K. (2017). Can cyberloafing and Internet addiction affect organizational information security?. *Cyberpsychology, Behavior, and Social Networking*, 20(9), 567-571.

Herrero, J., Urueña, A., Torres, A., & Hidalgo, A. (2019). Smartphone addiction: psychosocial correlates, risky attitudes, and smartphone harm. *Journal of Risk Research*, 22(1), 81-92.

Hinduja, S., & Ingram, J. R. (2009). Social learning theory and music piracy: The differential role of online and offline peer influences. *Criminal Justice Studies,* 22(4), 405-420.

HM Government. (2010). A Strong Britain in an Age of Uncertainty:The National Security Strategy. Retrieved from: https://webarchive.nationalarchives.gov.uk/20121018134855/http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf (accessed 7th July 2019).

HM Government. (2016). National Cyber Security Strategy 2016-2021. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (accessed 1st June 2019).

Holt, T. J., Brewer, R., & Goldsmith, A. (2018). Digital drift and the “sense of injustice”: Counter-productive policing of youth cybercrime. *Deviant Behavior*, 1-13.

Hoyle, R. H., Stephenson, M. T., Palmgreen, P., Lorch, E. P., and Donohew, R. L. (2002). “Reliability and Validity of a Brief Measure of Sensation Seeking.” *Personality and Individual Differences, 32(3), 401–414*

Ioanid, A., Scarlat, C. & Militaru, G. (2018). Social Networks: Friend or Foe?. Conference: 5th European Conference on Social Media (ECSM). Location: Limerick Inst Technol, Limerick, Ireland Date: Jun 21-22, 2018. *Proceedings of the European Conference on Social Media*, 85-92.

Jeong, W. (2009). The Recent Situation of Cyber Crime and the Legal Measurements. *Hongik University Legal Research Center,* 10(1), 195-224.

Jun. W. (2015). A Study on Relationship between Internet Addiction and Vocation. *Journal of Creative Information Culture*, 1(2), 87-91.

Jun. W. (2016). An Analysis Study on Correlation Between Dual-income Family and Internet Addiction of Children. *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology,* 6(4), 81-88.

Jun, W. (2017). An analysis work on correlation of internet addiction and school age groups. Cluster Computing, 20(1), 879-882.
Lazhintseva, E. M., & Bochaver, A. A. (2015). Internet as a new environment for adolescents' deviant behavior. *Voprosy Psikhologii*, (4), 49-+.

Kim, H.B. (2012). A Study on the Music Therapy Approach For the Internet Addiction Crime. *Korean Association of Addiction Crime Review*, 2(2), 65-87.

Kim, H. B. (2013). The Study on the Relationship between Smart Phone Addiction and Cybercrime. *Korean Association of Addiction Crime Review,* 3(2), 1-21.

Kim, H. (2018). An Empirical Study on the Determinants (Game Characteristics, Psychological Characteristics, Environmental Characteristics) about Causes of Game Excessive Immersion. *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology,* 8(2), 319-329.

Kim, K. W., & Seo, J. W. (2012). Relationship analysis between adolescent’s internet addiction levels and cybercrime. *Journal of Korean Public Police and Security Studies,* 9(2), 23-43.

Kim, T. H., & Kang, M. S. (2010). Measuring the Effectiveness of Teaching and Actual Condition of Internet Ethics of the Undergraduate Students. *Journal of the Korea Institute of Information and Communication Engineering*, 14(5), 1257-1269.

Koob, G. F., & Volkow, N. D. (2016). Neurobiology of addiction: a neurocircuitry analysis. *The Lancet Psychiatry*, 3(8), 760-773.

Kostyunina, N, Y., Latypova, L. A. & Sirazeeva, A. F. (2018). Prevention of Students’ Victim Behavior on the Internet. 4th International Forum on Teacher Education (IFTE 2018). Location: Kazan Fed Univ, Kazan, Russia. May 22-24, 2018. *European Proceedings of Social and Behavioural*

Sciences, (45), 193-205.

Kuss, D., & Griffiths, M. (2015). *Internet addiction in psychotherapy*. Basingstoke: Palgrave Pivot. pp.1 -5

Kuss, D., D Griffiths, M., Karila, L., & Billieux, J. (2014). Internet addiction: A systematic review of epidemiological research for the last decade. *Current pharmaceutical design*, 20(25), 4026-4052.

Kuss, D. J., Griffiths, M. D., & Pontes, H. M. (2017). Chaos and confusion in DSM-5 diagnosis of Internet Gaming Disorder: Issues, concerns, and recommendations for clarity in the field. *Journal of Behavioral Addictions*, 6(2), 103-109.

Kuss, D. J., Van Rooij, A. J., Shorter, G. W., Griffiths, M. D., & van de Mheen, D. (2013). Internet addiction in adolescents: Prevalence and risk factors. *Computers in Human Behavior*, 29(5), 1987-1996.

Livingstone, S., & Bober, M. (2004). Taking up online opportunities? Children's uses of the Internet for education, communication and participation. *E-Learning and Digital Media*, 1(3), 395-419.

Lee, B. H. (2018). Explaining cyber deviance among school-aged youth. *Child Indicators Research,* 11(2), 563-584.

Lee, E. G. (2009). A Study on Factors of Juvenile's Victimization from Cybercrime through chatting. *Korean Journal of Victimology*, 17(1), 267-289.

Lee, T. Y., & Song, B. H. (2017). Smart-phone addiction and countermeasure: Focusing on ethics education. Korean Criminal Psychology Review, 13(1), 195-226.

Lee, Y. B. (2013). The improvement method of Internet ethics education for the prevention of Internet aftereffect. *Journal of the Korea Institute of Information and Communication Engineering*, 17(6), 1432-1440.

Levi, M., Button, M., & Whitty, M. (2017). *Economic Crime: Learning from Offender Methodologies, and Pathways into (and out of) Crime*. Portsmouth: University of Portsmouth. Available at: https://core.ac.uk/download/pdf/153572728.pdf (accessed 5th August 2019)

Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: a comparative analysis. *Scientometrics*, 106(1), 213-228.

Morris, R. G., & Higgins, G. E. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. *Journal of Criminal Justice*, 38(4), 470-480.

Morse, S. J. (2017). The science of addiction and criminal law. *Harvard review of psychiatry*, 25(6), 261-269.

Mueller, K. W., Dreier, M., Duven, E., Giralt, S., Beutel, M. E., & Woelfling, K. (2017). Adding Clinical Validity to the Statistical Power of Large-Scale Epidemiological Surveys on Internet Addiction in Adolescence: A Combined Approach to Investigate Psychopathology and Development-Specific Personality Traits Associated With Internet Addiction. *The Journal of clinical psychiatry,* 78(3), e244-e251.

Navarro, J. N., Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2014). Addicted to pillaging in cyberspace: Investigating the role of internet addiction in digital piracy. *Computers in Human Behavior,* 37, 101-106.

Neto, A. C. D. A., Eyland, S., Ware, J., Galouzis, J., & Kevin, M. (2013). Internet sexual offending: Overview of potential contributing factors and intervention strategies. *Psychiatry, psychology and law*, 20(2), 168-181.

Nykodym, N., Ariss, S., & Kurtz. K (2008). Computer addiction and cyber crime. *Journal of Leadership, Accountability and Ethics*, 35(1), 78-85.

Öze. N (2018). Complaints on 'Social Media Addiction' by it's Users. Paper presented at 5th European Conference on Social Media ECSM 2018. Reading: Academic Conferences and Publishing International Limited.

Park, C. S. (2012). A Constitutional Investigation on the Online Game Shutdown System. *Hanyang Law Association, Hanyang Law Review*, 23, 1.

Pontes, H. M., Kuss, D. J., & Griffiths, M. D. (2015). Clinical psychology of Internet addiction: a review of its conceptualization, prevalence, neuronal processes, and implications for treatment. *Neuroscience & Neuroeconomics*, 4, 11-23.

Potenza, M. N. (2014). Non-substance addictive behaviors in the context of DSM-5. *Addictive behaviors,* 39(1), 1-2.

Rammstedt, B., & John. O., P. (2007). Measuring Personality in One Minute or Less: A 10-Item Short Version of the Big Five Inventory in English and German. *Journal of Research in Personality*, 41(1), 203–212.

Rashid, A., Baron, A., Rayson, P., May-Chahal, C., Greenwood, P., &

Walkerdine, J. (2013). Who am i? analyzing digital personas in cybercrime investigations. *Computer*, 46(4), 54-61.

Reyns, B. W. (2019). Online pursuit in the twilight zone: cyberstalking perpetration by college students. *Victims & Offenders*, 14(2), 183-198.

Ryding, F. C., & Kaye, L. K. (2018). "Internet addiction": A conceptual minefield. *International journal of mental health and addiction,* 16(1), 225-232.

Santos, V. A., Freire, R., Zugliani, M., Cirillo, P., Santos, H. H., Nardi, A. E., & King, A. L. (2016). Treatment of Internet addiction with anxiety disorders: Treatment protocol and preliminary before-after results involving pharmacotherapy and modified cognitive behavioral therapy. *JMIR research protocols*, 5(1), e46.

Shaw, M., & Black, D. W. (2008). Internet addiction. *CNS drugs*, 22(5), 353-365.

Shin, H. (2011). A Study on the Introduction of the Private Investigation Service System. *Korean Association of Addiction Crime Review*, 1(1), 139-165.

Solmaz, M. H., & Saygili, S. (2011). An adolescent case with Internet addiction and hacking: how are we dealing with this diverse spectrum of disorder?. General hospital psychiatry, 33(4), e15

Starcevic, V. (2013). Is Internet addiction a useful concept?. *Australian & New Zealand Journal of Psychiatry*, 47(1), 16-19.

Starcevic, V., & Aboujaoude, E. (2017). Internet addiction: Reappraisal of an increasingly inadequate concept. *CNS spectrums*, 22(1), 7-13.
Tikhonov, M. N., & Bogoslovskii, M. M. (2015). Internet addiction factors. Automatic Documentation and Mathematical Linguistics, 49(3), 96-102.

Tomažič, T., & Bessa-Vilela, N. (2017). Ongoing criminal activities in cyberspace: From the protection of minors to the Deep Web. Revija za kriminalistiko in kriminologijo, 68(4), 412–423.

Toncheva, A. V. (2012). Diagnosis of cyber-communication addiction. *Naukovedenie*, 4,
2-3.

Yu, T. K., & Chao, C. M. (2016). Internet misconduct impact adolescent mental health in Taiwan: The moderating roles of internet addiction. International *Journal of Mental Health and Addiction*, 14(6), 921-936.

Sussman, N., & DeJong, S. M. (2018). Ethical considerations for mental health clinicians working with adolescents in the digital age. *Current psychiatry reports,* 20(12), 113.

Wallace, P. (2004). *The Internet in the workplace: How new technology is transforming work*. Cambridge: Cambridge University Press.

Wall, D. S. (2008). Cybercrime and the culture of fear: Social science fiction (s) and the production of knowledge about cybercrime. Information. *Communication & Society*, 11(6), 861-884.

Wan, C. (2009). A Study on the Cyber Infringement of Human Rights and the Remedy. *The Justice*, 109, 7-42.

Appendix 1. Summary of results

Study (Year)	Title	Author(s)	Main Aims	IA Cybercrime narrative	Sample [Design/Method]	Research Field(s)	Main Results
2011	An adolescent case with Internet addiction and hacking: how are we dealing with this diverse spectrum of disorder?	Solmaz, & Saygili	Present a case study of IA. Study aimed to provide evidence supporting inclusion of IA being included in the DSM V as a clinical disorder.	Case study gives evidence from family members and clinicians of the subject suffering withdrawal symptoms when unable to access the internet, including anger and intense anxiety. The subjects internet use caused detriment to other areas of his life, including social relationships and educational success. The development of IA in this case was driven by the subjects membership of an online hacking community. Psychiatric treatment combining therapy and drugs	A case study of a 16-year-old Turkish male adolescent who was a first-year high school student struggling with academic failure, despite previously being a successful in education. It was claimed that this individual was suffering from IA which had developed after he had joined a hacking group.	Psychiatry	IA appeared to be caused by a need for constant connectivity to the subjects hacking community. This group appeared to have significant social significance to the male. IA resulted in emotional and social dysfunctions. It is suggested that IA may have comorbidity with other disorders and may be resistant to treatment. Psychiatric treatment was effective in treating the behaviour issues the subject suffered from. The treatment also redirected the male from his hacking community into offline social groups.
2013	Internet sexual offending: Overview of potential contributing factors and intervention strategies	Neto, Eyland, Ware, Galouzis & Kevin	To explore the factors that potentially contribute to Internet Sexual Offending and what intervention strategies may be effective.	The paper strongly links online sexual offending to low self-control and deficits in self-regulation. Offending behaviour may be conditioned, but it also may be a coping strategy for life stress. Internet Addiction is proposed as a possible cause of dysfunctional sexual behaviour online. The paper cites an example of an Australian case (downloading indecent images of children) where	Literature review conducted by Australian researchers with an international outlook.	Forensic Psychology	The paper proposes that psychologists seeking to reduce offending of online sex offenders should help them develop stronger impulse control. It is suggested that clinicians should understand underlying patterns of internet use to best implement intervention strategies. A need to make the individual aware of the harm caused by the production of all sexual images of children is highlighted; challenging a tendency of offenders to intellectualise their behaviour. However, the role of the sex

				the defendant claimed he was looking at the images because of an Internet Addiction, a compulsion caused by depressive illness.			offender in ensuring no further offending is stressed. The researchers recommend stronger international ties between law enforcement agencies and publicity of prosecutions, to ensure online offenders are aware of the potential consequences of their behaviour.
2014	Addicted to pillaging in cyberspace: Investigating the role of internet addiction in digital piracy	Navarro, Marcum, Higgins & Ricketts	(i)To study was whether IA was correlated with digital piracy (ii) To establish if deviant peer association increased likelihood of engaging in digital piracy (iiI) To test previous research findings that piracy was more common among males.	The study recognised IA was emerging as an explanation for deviant behaviour online and wished to test the hypothesis that IA ("Internet Related Problems") would increase rates of perpetration of digital piracy. Previous research linking impulsive behaviour to digital piracy was noted. The possible link between IA and impulsive online behaviour highlighted.	A between subjects design with 1617 American students from grade 9 -12 (14-18yrs old average age 15.77) from a rural county in western North Carolina. 49% of the sample was male, 72% white. The study used three measures; a three item piracy scale, a measure of deviant peer association, both derived by the researchers and also used an existing measure of IA (Armstrong, Phillips, & Saling, 2000).	Human Computer Interaction	13% of the sample engaged in software piracy, 15% engaged in music piracy, and 29% movie piracy. IA was correlated with software piracy but not music or movie piracy. As an individual associates with more deviant peers the likelihood of software, music and movie piracy increases. Male sex was associated with software and movie piracy, but not music. White students were more likely to pirate music than non-white students. Social learning theory appears to explain behaviour across different forms of digital piracy while IA may be a partial factor in some cases (software).
2015	Internet Addiction Factors	Tikhonova & Bogoslovskii	To explore factors influencing individuals developing IA in a Russian context.	Cybercrime defined as fraud, sexual exploitation, vandalism, cyberbullying, and other manifestations of aggression and hostility. IA is linked to these types of online offending.	Literature review. The paper mostly draws from Russian sources, giving a view of a Russian perspective on IA	Human Computer Interaction Psychology	Narrative links IA with several social issues, including cybercrime. Very little evidence is provided of a link between IA and cybercrime, however this is acknowledged by the paper, stating that in the Russian context research on any aspect of the internet is rare. The paper also criticises a lack of consistency in measures used to research IA in Russia. The paper does discuss research into at medical context that IA causes negative emotional states, issues with socialising and a lack of

							personal responsibility. The paper also cites Russian research suggesting that 75% of IA suffers also have issued with alcohol abuse and drugs.
2016	Internet misconduct impact adolescent mental health in Taiwan: The moderating roles of internet addiction	Yu, & Chao	(i) Explore the impact of cyber bullying, cyber pornography, and Internet fraud on physical and mental health (ii) To establish the influence of IA as a moderating factor on the variables (bullying, pornography, fraud) on the outcome (quality of physical and mental health)	IA described as a" global major mental health problem". IA connected to cyber bullying but not cyber crime.	'Probability-proportionate-to-size sampling method' was used to systematically draw a random sample of 150 high schools in Taiwan, from which classes were randomly selected. 8480 students (49.3% male) from these classes, aged between 13 and 18 (mean 16.45, SD 0.93) completed self-report surveys. The instruments, derived by the researchers aimed to measure; cyber bullying, cyber pornography use, cyber fraud, IA, and physical and mental health, and used four-point Likert scale.	Human computer interaction Psychology	IA had a significant influence on physical and mental health, which was poorer on average than non-IA sufferers. 25.9% of the variance in physical and mental health was linked to the condition. IA was found to be a moderator of the influence cyber bullying and cyber pornography on physical and mental health; but not of cyber fraud. The study suggests that an interaction between IA and online bullying/online pornography viewing may exacerbate negative effects of these behaviours.
2017	Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours.	Haddlington	To explore the relationship between risky cybersecurity behaviours, attitudes towards cybersecurity in a business environment, Internet addiction, and impulsivity.	IA among employees is a significant predictor for online behaviours that cause a security vulnerability. This is linked with impulsive behaviour. IA represents a cyber security vulnerability.	A between subjects design. 538 participants, 297 Female, in part-time or full-time employment based in the UK completed an online questionnaire. The survey included four scales: Abbreviated impulsiveness scale (ABIS) Online cognition scale (OCS) Risky cybersecurity behaviours scale (RScB) Attitudes towards cybersecurity and cybercrime in business scale (ATC-IB)	Psychology	Internet Addiction was a significant predictor for risky cybersecurity behaviours. Attentional and motor impulsivity were both significant positive predictors of risky cybersecurity behaviours, with non-planning being a significant negative predictor.
2017	An analysis work on correlation of internet addiction and school age groups.	Jun	To identify the factors related to IA and examine how psychiatric symptoms of the condition may present in	IA is a source of serious social problems and has a negative impact on the mental health teenagers	The study analysed data that had been gathered in a four-year (2011–2014) national survey on internet addiction	Psychiatry Psychology	A significant correlation found IA to be more common in older school groups. Overall between 9 and 10.3% of the population

			Korean adolescents, controlling for demographic and internet access related factors.	and is linked to anxiety, stress, impulsivity, depression and a lack of self-control. The study linked IA to copyright infringement, hacking and cyber bullying, as all being examples of negative impacts of digital technology. However, the paper but did not explicitly cite research showing a connection with criminality and the condition, and the study itself did not explore a connection.	in Korea. Analysing correlation between IA and mental health issues, the study cross analysed five different age groups, starting at Kindergarten and going up to University Students. The size of the population studied varied between over 4,000 and just under 6,000 students depending on year. Details of what measure of IA or other data gathered by this national survey are not stated. It is not stated what the relative sizes of the age groups are, or any other demographic information.		studied was believed to suffer from IA. The study suggests public policy should be to engage students in IA prevention and treatment programs at an early age. The paper states that such a measure was not present in Korea at that time. The study also argued that IA treatments should consider the age of the students and prepare efforts appropriate for the different ages of students suffering with the condition.
2017	Ongoing criminal activities in cyberspace: From the protection of minors to the Deep Web.	Tomažič, & Bessa-Vilela	To explore cybercrime from the context of child and adolescent protection from a Slovenian perspective.	IA narrative is balanced with the paper calling for the condition to be taken into consideration in the creation of public policy. Potential for negative impacts on sufferers lives, however disputed nature of condition discussed.	The study utilised a literature review of cybercrime factors followed by a statistical analysis of police data regarding cybercrimes committed in Slovenia between 2011 and 2015.	Criminology Public policy	The paper discusses the disputed nature of IA, but highlights evidence of psychosocial maladjustment caused by the condition impacting individuals and society in multiple contexts. The paper calls for greater awareness of IA in public policy in Slovenia. The paper also suggests that public policy must respond to the psychological impact of the condition to protect children and young people. Practical suggestions are made regarding the roles of parents, teachers, the education system, peers, government agencies, private industry and wider society, in better tackling issues caused by IA.

2018	Prevention of Students’ Victim Behavior on the Internet	Kostyunina, Latypova & Sirazeeva	(i) Evaluate the effectiveness of a program developed to prevent students’ engaging in vulnerable online behaviour. (ii) Evaluate the effectiveness of diagnostic tools to prevent students’ engaging in vulnerable online behaviour.	IA among students can cause online victimisation. IA was indirectly linked to anti-social behaviour and violation of social norms and ethics, impulsive emotional reactions, impatience, anger, carelessness and poor judgement of situations	A between subjects design. 127 participants, all students of the Institute of Psychology and Education of Kazan Federal University in Russia (aged 18-21) Schubert's “Readiness for Risk”scale Cyber-Communication Addiction scale "Addiction to victim behavior" Scale	Psychology Education studies	The influence of the internet can have complex effects on the personal characteristics of users. These can be both positive and negative. ‘Cyber-addiction’ was found to be a form of addictive behaviour associated with internet use, which caused students increased likelihood of online victimisation. Preventative educational inputs by the university were effective in reducing the proportion of students with high or medium online addictive behaviours from 19.6% to 9.4%.
2018	Explaining cyber deviance among school-aged youth.	Lee	Expand on prior research into factors causing individuals to become engaged in deviant online activity. The study explored cyber-deviance among South Korean adolescents, which the author suggests is under researched context.	IA is highlighted but not directly researched. Narrative suggests IA effected adolescents may be unable to function effectively at home and school, suffer from psychological issues, including depression, suicidal ideation and avoidance of social situations. It is also suggested that IA sufferers may be more likely to exposed to sexual online content and sexually solicited. These claims are supported by citations. Low-self control was a significant factor in online offending, but less significant than peer influence. The researcher suggests both factors should be considered in public policy.	Convenience sample of 779 students (50.7% male) attending upper elementary and middle schools (10 to 16 years old) in the public school system of a medium-sized urban area in South Korea. Study explored bivariate relationships between four types of deviant behaviours online, low self-control, deviant peer association, technology related and sociodemographic variables. Study was correlational and did not claim causal relationships.	Psychology	Ownership of digital technology and proficiency in using those devices was associated with higher levels of online deviant behaviour (media piracy, software piracy, online harassment, and computer hacking). Time spent online in various forms (except being online for educational reasons) were associated with deviant behaviours. Older members of the sample and males were more likely to engage in online deviant behaviours. Association with peers engaging in deviant behavours (on or offline) increased chances of youth offending by 24% for media piracy, 21% for software piracy, 15% for online harassment, and 23% for computer hacking Low self-control was only

							significantly correlated with online harassment and computer hacking. Family structure/background had no statistically significant relationship with deviant online behaviour
2018	Ethical considerations for mental health clinicians working with adolescents in the digital age.	Sussman & DeJong	(i)Explore ethical issues, relating to digital technology use, facing mental health professionals working with adolescents. (ii) Consider how established ethical principles in psychology can be applied	Within the paper academic evidence of IA being linked to victimisation is explored. While various types of victimisation are discussed, only suggestion of a link between cyberbullying and trolling victimisation and IA is evidenced.	Literature review, written from an American mental health perspective. American Academy of Child and Adolescent Psychiatry ethical frameworks are presented. A series of vignettes exploring modern ethical issues in the context of this framework are presented.	Psychiatry Clinical Psychology	Writers call for clinicians working with adolescents to be more mindful of how digital technology can interact with metal health. The writers argue that the first challenge in this area is a recognition by mental health professionals of emerging issues, and to keep updated with changes to technology. It is suggested that existing ethical frameworks are able to be applied in the best interests of the child, once the issues are recognised.
2019	Smartphone addiction: psychosocial correlates, risky attitudes, and smartphone harm.	Herrero, Urueña, Torres, & Hidalgo	Expanding on relationship between personality traits, social relationships and levels of smartphone use and IA (to smartphones). The study sought to explore how these characteristics in combination with IA suffering smartphone users influences risky behaviours that compromise cybersecurity. Research questions: (i) "What are the correlates of smartphone extensive use and addiction?" and (ii) "what is the relationship among smartphone extensive use and addiction, risk attitudes and perceptions of smartphone use and smartphone harm?"	IA may cause those with the condition to engage in risky online behaviour. This increases their chances of becoming a victim of cybercrime.	Between subjects design, correlational descriptive. The study used data from the 'Cybersecurity and Confidence in Spanish Households national survey' (2015). This data included online psychometric questionnaires and data obtained by scanning Android smartphones for malware. Participants were 526 smartphone using Spanish residents (51.9% male) with home internet access. The sample was screened to be representative of the total Spanish population. Study utilised the 'Smartphone Addiction Symptoms Scale' (Bian, & Leung, 2015), An abbreviated version of the	Psychology	The only socio-demographic variable positively correlated with IA was being female. Neuroticism and a propensity to take risk and lower levels of social support were positively correlated with IA symptoms. Those showing high addiction symptoms and low levels social support reported higher risky attitudes/behaviour in smartphone use. Study noted that directionality of relationships could not be claimed.

					Big Five Inventory (Rammstedt & John, 2007), The Brief Sensation-Seeking Scale (Hoyle et al, 2002) and others.		
2019	Online Pursuit in the Twilight Zone: Cyberstalking Perpetration by College Students	Reyns	Examined the relationship between students' cyberstalking behaviors and their participation in other "misdeeds" online	Literature review in study suggested that cyberstalking perpetration was associated with low self-control and impulsive behaviour. IA was suggested by the researches as a possible contribution factor to this behaviour. Evidence presented was not directly linked to cyberstalking, but did highlight impulsive behaviour and low self-control is associated with the condition.	Between subjects design. The data utilized in the study was collected in 2009 through a self-report survey administered to a probability sample of college students from a large urban university in the Midwest USA. The analytic sample included 759 students, 61% female, 87% White, and 57% nonsingle. Average age of 20 years old.	Criminology / Victimology	Low self-control was a significant predictor of cyberstalking perpetration and online pursuit behaviours Students with lower self-control were over twice as likely to perpetrate cyberstalking in comparison to peers with higher levels of self-control. Receiving an explicit photo increased the odds cyberstalking perpetration over two times.