



International Journal of Technology, Policy and Management

ISSN online: 1741-5292 - ISSN print: 1468-4322

<https://www.inderscience.com/ijtpm>

Multifaceted issues of cybercrime in contemporary era

Tansif Ur Rehman

DOI: [10.1504/IJTPM.2025.10064820](https://doi.org/10.1504/IJTPM.2025.10064820)

Article History:

Received: 23 July 2023

Last revised: 25 February 2024

Accepted: 25 February 2024

Published online: 02 April 2025

Multifaceted issues of cybercrime in contemporary era

Tansif Ur Rehman

Department of Criminology,
University of Karachi,
Karachi, 75270, Pakistan
Email: Tansif@live.com

Abstract: The internet is undoubtedly the most creative development of the modern era since it continues transforming practically anyone's everyday life worldwide. Billions of people are connected to the internet, and many more join daily. Simultaneously, as internet advancements continue to thrive, criminals have devised methods to use such developments in almost the same manner they would use any weapon for an illegal act. Identifying and settling an infraction is much more challenging than typical crimes. Every day, cybercrime units worldwide get thousands of reports. Cybercriminals are inventive, well-organised, and significantly more skilled than traditional criminals. They use their tools well, work more diligently, and concentrate on identifying new weaknesses and evading discovery. The most pervasive types of cybercrime are elaborated in this research. The theory of planned behaviour (TPB) is also discussed, and the proposed approach is validated using the systematic review method.

Keywords: cyberstalking; cyberterrorism; cyber frauds; pornography; systematic review.

Reference to this paper should be made as follows: Rehman, T.U. (2025) 'Multifaceted issues of cybercrime in contemporary era', *Int. J. Technology, Policy and Management*, Vol. 25, No. 1, pp.94–116.

Biographical notes: Tansif Ur Rehman is working as a Teaching Associate at the Department of Criminology, University of Karachi, Pakistan. He has been a reviewer for various reputed national and international journals for the last three years. He has 94 publications (papers and chapters), seven books, over 22 years of teaching, and 16 years of research experience.

1 Introduction

Cybercrime can indeed be understood in various ways, as in the broadest sense, it encompasses every wrongdoing using a computer network (Cripps, 2021; EmBroker, 2021; McQuade, 2008). Few definitions encompassing the subject matter are cited. According to Cybercrime (2021d), it refers to criminal behaviour (like distribution of child pornography, theft, or fraud) performed to unlawfully access, transmit, or manipulate data through a computer. According to the Cybercrime (2021e), cybercrime is an internet-related crime, such as stealing someone's data or attacking their system from viruses.

It is a type of crime done via the internet and computer (Cybercrime, 2021b). According to Cybercrime (2021c), it is a criminal act committed through the internet or a computer program. Cybercrime (2021a) states that a computer system is used to advance illicit activities like invading privacy, stealing identities and intellectual property, or fraud. It has, particularly over the internet, increased prominence in lockstep with the computer. Hackers have increasingly utilised sophisticated phishing email techniques since the outbreak of COVID-19. The malicious actors pretend to be the WHO (PurpleSec, 2021).

The global cost of cybercrime is expected to reach \$6 trillion by 2021, and it is projected to increase to \$10.5 trillion by 2025. In 2022, the global information security industry is forecast to reach \$170.4 billion due to the projected increase in cybercrime. 61% of cybersecurity experts feel their team needs to be more staffed. The cybersecurity skills gap will remain a significant issue, resulting in 3.5 million unfilled jobs by 2021 (Packetlabs, 2021).

While it is easy to characterise cybercrime as simply the behaviour of a lone entity, although this is valid for some offenses, the actuality of cybercriminals is relatively diverse (Gillespie, 2019; Yar and Steinmetz, 2019). Due to the lucrative nature of cybercrime in the modern period, many thousand gangs have formed (Austin, 2020; Johansen, 2020; Troia, 2020; The Daily Swig, 2021).

It is self-evident that as individuals' reliance on technology increases, they become more exposed to cybercrime (Marsh and Melville, 2019; Steinberg, 2019), which may adapt to create new issues (Hufnagel and Moiseienko, 2019). Understanding how individuals perceive the severity of cybercrime that they have either experienced or could potentially experience is crucial (Abaimov and Martellini, 2020; Bandler and Merzon, 2020; PurpleSec, 2021). An example of illegal activity is sending emails that demand users to provide their bank information, yet nearly everyone with an email account has received an email asking them to verify their banking details (Azevedo, 2018; Bancroft, 2019; Carlson, 2019).

Another challenge is identifying cybercrime victims or unaware they have been attacked (Edwards, 2019; Sangster, 2020; Schober and Schober, 2019). Most computer users understand the importance of installing firewalls and antivirus software (Graham and Smith, 2019; Kim, 2018; Littler and Lee, 2020). It is rare for someone to know that their application prevented a virus or attempted intrusion (Hutchings, 2013; Packetlabs, 2021). Smith (2018) reported that during the Black Hat and Def Con hacking conferences held in August 2018, it was disclosed that hacking and manipulating patients' vital signs, insulin pumps, and pacemakers in real time was possible. The Ponemon Institute USA (2018) notes that 64% of firms in US have faced successful endpoint assaults in recent years.

Cybercrime prevention mainly depends on government agencies, commercial organisations, and internet users adopting a security culture (Abaimov and Martellini, 2020; Sangster, 2020; Steinberg, 2019). Prevention will always be the best defence, and significant reforms in enforcement and law will be necessary (Gillespie, 2019; Glenny, 2012; Lavorgna, 2020; Willems, 2019). Education and awareness among people will go a long way toward preventing individuals from falling victim to cybercrime and mitigating associated hazards (Benson and McAlaney, 2019; Graham and Smith, 2019; Lusthaus, 2012).

2 Research question

What are the multifaceted cybercrime issues in the contemporary era, and how can they be effectively addressed?

3 Research justification

- 1 **The growing threat of cybercrime:** Cybercrime has become an increasingly pervasive and sophisticated threat in the contemporary era. It poses significant challenges to individuals, businesses, governments, and global security. Research on the multifaceted cybercrime issues is crucial to understanding the nature, extent, and impact of cyber threats and developing effective strategies to combat them.
- 2 **Rapid technological advancements:** The evolution of technology has led to new opportunities for cybercriminals to exploit vulnerabilities and launch sophisticated attacks. Understanding the multifaceted issues of cybercrime in the context of contemporary technology trends, such as artificial intelligence, the internet of Things, and cloud computing, is vital to staying ahead of cyber threats and developing proactive defence mechanisms.
- 3 **Legal and regulatory complexity:** Cybercrime operates across national borders, making it a complex challenge for law enforcement and legal systems. Research on the multifaceted cybercrime issues can shed light on the legal and regulatory gaps and challenges in addressing cyber threats. It can provide insights into developing effective international cooperation frameworks, harmonising cyber laws, and strengthening legal mechanisms to combat cybercrime.
- 4 **Socioeconomic implications:** Cybercrime has wide-ranging socioeconomic implications, including financial losses, reputational damage, privacy breaches, and social unrest. Research on the multifaceted issues of cybercrime can analyse its impact on individuals, businesses, and society. It can inform the development of cybersecurity strategies that protect against cyber threats and mitigate the socioeconomic consequences of cybercrime.
- 5 **Protection of critical infrastructure:** Critical infrastructure, such as power grids, transportation systems, and financial networks, are increasingly interconnected and reliant on digital technologies. The multifaceted cybercrime issues pose a significant risk to the security and resilience of critical infrastructure. Research can explore the vulnerabilities, potential attack vectors, and mitigation strategies specific to protecting critical infrastructure from cyber threats.
- 6 **Privacy and data protection:** Cybercrime often compromises personal data and causes privacy breaches. Research on the multifaceted cybercrime issues can examine the challenges and implications of data breaches, identity theft, and privacy violations. It can inform the development of privacy-enhancing technologies, data protection regulations, and best practices for individuals and organisations to safeguard personal information in the digital realm.

- 7 **International cooperation and collaboration:** Cybercrime transcends national boundaries, requiring international cooperation and collaboration for effective response and prevention. Research on the multifaceted cybercrime issues can explore the challenges and opportunities for international cooperation, information sharing, and joint efforts in combating cyber threats. It can contribute to developing frameworks for international collaboration, capacity-building initiatives, and sharing best practices among nations.
- 8 **Ethical considerations:** Research on the multifaceted cybercrime issues involves ethical considerations, such as the responsible use of technology, privacy rights, and data protection. It can contribute to discussions on ethical frameworks for cybersecurity practices, responsible conduct in cyberspace, and the ethical implications of emerging technologies concerning cybercrime.

By researching the multifaceted issues of cybercrime in the contemporary era, policymakers, law enforcement agencies, cybersecurity professionals, and other stakeholders can gain valuable insights to inform their decision-making processes, policy development, and effective measures to combat cyber threats. The research can strengthen cybersecurity practices, enhance legal frameworks, protect critical infrastructure, and safeguard individuals and organisations in the digital landscape.

4 Research focus

This research highlights the four most pervasive types of cybercrime in the contemporary era, i.e., cyberterrorism, cyber fraud, illegal pornography, and cyberstalking. As cybercrime is a multifaceted problem, a multidimensional approach is required to analyse the subject matter of the issue. Consequently, the systematic review technique was chosen, and the corresponding processes were followed.

5 Research objectives

- 1 To explore the aspects of cyberterrorism in the contemporary era.
- 2 To highlight the two major types of cyber frauds, i.e., financial and romance frauds.
- 3 Critically analyse pornography and its detrimental effects on children, teens, and adults.
- 4 To discuss the effects of cyberstalking along with its characteristics.

6 Research methodology

This study used a systematic review method, which involved determining the research objectives and conducting an extensive literature review (Komba and Lwoga, 2020). The research findings were then categorised based on their content (Petticrew and Roberts, 2006) and included in the study by organising them as headings (Pawson et al., 2005).

The study flow was established by evaluating the classified information and titles (Rahi, 2017), ensuring the research subject's integrity (Victor, 2008).

7 Literature review

The proliferation of technology-enabled gadgets and internet capabilities creates an unavoidable need for computer-assisted crimes. However, awareness of cybercrime's ubiquity and study into the causes and repercussions of these crimes are minimal. As a result, a thorough literature assessment was required to serve as the foundation for the presented work.

A literature review possesses a variety of distinguishable traits and imperatives. The first need is for the reviewer to provide a thorough yet pragmatic assessment of the material under consideration. By engaging with and criticising previous research, the researcher must balance demonstrating criticality through inquisitive and considered arguments about the assumptions, theories, and methods used and simultaneously acknowledging the validity of the study's findings, insights, and strengths (Harris, 2019).

Second, literature reviews should go beyond a descriptive recitation of previously published material and contain a thread – a train of thought – that gradually leads to the study subject for which the review is being done. It involves finding gaps in the existing body of knowledge (Purssell and McCrae, 2020).

A third aspect, which receives less emphasis, is that evaluations continue throughout a research project instead of the usual notion that they commence at the beginning and conclusion (Hempel, 2019). The review will evolve as the study proceeds, necessitating improvements and alterations. Empirical findings may drive the study differently, requiring revisions to earlier arguments. Because discoveries occur regularly, the research must reflect and be as up-to-date as feasible (Fink, 2019).

7.1 *Theory of planned behaviour*

LaMorte (2019) believes this theory was developed to encompass all behaviours that enable humans to exhibit self-control. The central aspect of this paradigm is behavioural intent, where behavioural motivations are shaped by the response to the probability of achieving the desired outcome and the contextualised evaluation of the cost/benefit associated with that outcome.

The respective theory has been successfully used to forecast and clarify various health habits and intentions, including drug use, smoking, breastfeeding, alcohol consumption, and healthcare utilisation. According to the notion, behavioural success is contingent upon ability (behavioural control) and motivation (intention) (Apau and Koranteng, 2019; Jafarkarimi et al., 2016). It distinguishes between three forms of belief-behavioural, normative, and regulation. The respective theory comprises six components that precisely control an individual's behaviours.

- 1 attitudes
- 2 behavioural intention
- 3 perceived behavioural control
- 4 perceived power

- 5 social norms
- 6 subjective norms.

8 Most pervasive types of cybercrime

1 Cyberterrorism

The main uses of the internet by terrorists, according to scholars like Abaimov and Martellini (2020); Austin (2020); Bancroft (2019); Hufnagel and Moiseienko (2019); Jones (2005); Lavorgna (2020); Leukfeldt and Holt (2019); Littler and Lee (2020); Marsh and Melville (2019); Martellozzo and Jane (2017); Willems (2019); Yar and Steinmetz (2019) are:

i *Propaganda*

The internet, particularly after the invention of Web 2.0, is a very cheap way to get a message out. The message can also be presented uncritically, which would not occur through other media. The full extent of this has been seen through the respective videos posted on YouTube, which often show the cruel actions of terrorists. Recruitment videos have also been uploaded, which present a significantly distorted view of the objectives of the terrorist organisation to portray the belief that their activities are in some way or appropriate.

ii *Fundraising*

Terrorism is an expensive business with a political goal that people are sympathetic to, and there will be people who will be prepared to contribute to the cause. Having a 'global reach' became much more accessible because a fundraising site can be formed and disseminated through email, social media, and hyperlinks. Several online payment systems allow people to donate money. The internet also allows anonymous money transfers, which could be particularly attractive in the context of terrorism, as it will allow people to donate money without fearing impacts.

iii *Information dissemination*

It is slightly different from propaganda; information dissemination would be helpful to the cause rather than a specific group. The internet has numerous examples of bomb-making instructions and terrorism-aiding manuals. This dissemination intends not necessarily recruitment in a particular group but rather empowering those sympathetic to the cause to develop their strategies for causing terror. Dissemination of such information poses a real risk to society, as it allows people to produce improvised explosive devices cheaply for any cause, potentially widening the likelihood of an attack.

iv *Secure communication*

The internet allows entirely new communication methods, for example, VoIP (Voice Over internet Protocol) software packages such as FaceTime, Facebook, WhatsApp, and Skype. An advantage of this is that an anonymous email address can be created and linked to an anonymous Skype address. Therefore, the chance that authorities are aware of the existence of the call may be remote.

2 Cyber frauds

A *Variety of financial frauds*

On the internet, a wide range of scams is conducted. Each year, new types emerge (Azevedo, 2018; Benson and McAlaney, 2019; Hufnagel and Moiseienko, 2019; Lavorgna, 2020). A detailed examination of fraud reveals seven distinct categories.

- i **Fraud through low-level deception** includes schemes such as advertising to sell non-existent or counterfeit goods.
- ii **Fraud via built narrative application:** This is the stage at which a relationship between the fraudster and victims is formed.
- iii **Participation via employment-based strategies:** This may include advertising a position that needs to complete a course or a fee-based application.
- iv **Fraud through implying an obligation:** This scam demands the user's reaction to work. It might be an inadvertent subscription to a website that needs the user to phone a specific number to be paid.
- v Information acquisition via ostensibly legitimate appeals: This includes both spoofing and phishing.
- vi Monetary benefit via retailer and consumer subjugation primarily refers to internet auction fraud.
- vii **Financial advantage by promotional strategies:** This category includes charitable frauds and Pyramid schemes, which are, of course, fraudulent.

B *Romance frauds*

In recent years, there has been a resurgence in the target of individuals through romance websites (Graham and Smith, 2019; Martellozzo and Jane, 2017). One of the most significant growth areas globally is dating portals (Benson and McAlaney, 2019). People's desire to communicate with each other romantically allows people to be defrauded (Hudak, 2019; Leukfeldt and Holt, 2019). There are thousands of complaints concerning romance fraud, with losses of millions of dollars annually worldwide (Gillespie, 2019; Steinberg, 2019; Yar and Steinmetz, 2019).

3 Pornography

In recent years, the digital porn industry has proliferated due to increased internet connectivity and technical advancements, notably in video streaming, which enables people to see media continually, often a video, without downloading it (Dwulit and Rzymiski, 2019; Wilkinson, 2017). As a result, it is unsurprising that sexual content is now pervasive and easily accessible online, even though avoiding deliberate and inadvertent access to it might be challenging on occasion (Wright et al., 2018; Zhang and Jemmott, 2015).

Although it has a long history, it has undoubtedly hit a record high due to modern technology (Dwulit and Rzymiski, 2019). It is currently available in a virtually endless sexual variety online for free, and by any gadget with an online connection, primarily in the videos, that has been claimed to become the most sexually appealing type of adult material (Laan and Everaerd, 1995; Koukounas and Over, 1997). The convenience at

which internet porn could reach individuals and arousal power suggests that it could function as a supranormal stimulant (Dwulit and Rzymiski, 2019; Goodwin et al., 2015; Hilton, 2013; Park et al., 2016). Nevertheless, disagreements exist on its precise impact on its users. According to various research, long-term usage is often associated with reduced libido, erectile dysfunction, a greater inclination to porn than sexual interaction with an actual person (Dwulit and Rzymiski, 2019; Steele et al., 2013; Sun et al., 2014), and decreased relationship and sexual satisfaction (Bridges and Morokoff, 2011; Perry, 2016; Poulsen et al., 2013; Wery and Billieux, 2016; Zillmann and Bryant, 2006).

Because of its non-recognition as a disorder under the DSM-5 and ICD-10, researchers refer to it as; self-perceived pornography addiction” (Duffy et al., 2016; Grubbs and Perry, 2019; Sniewski et al., 2018). Neurobiological evidence suggests that it shares similar mechanisms with chemical substance addictions and thus could fit within the general addiction framework (Brand et al., 2014; Brand et al., 2016; Kuhn and Gallinat, 2014; Klucken et al., 2016; Love et al., 2015). However, some disagreements and substitute models that rely on compulsive behaviour, impulsive behaviour, or ethical dissonance have been proposed to account for the high usage of porn (Grubbs and Gola, 2019; Ley et al., 2014).

A *Adult pornography*

Adult pornography is also gaining popularity internationally, i.e., pornography that includes adults (Nair, 2018) exclusively. There are three primary issues associated with adult pornography, which are all somewhat interrelated:

- i **Obscene publications:** While many nations permit adult pornography, some believe publishing essays or visuals is ethically reprehensible.
- ii **Revenge porn:** An escalating kind of conduct wherein a person purposefully uploads film or photographs to a social platform to enable individuals to seek vengeance on former spouse and pals.
- iii **Extreme pornography:** Possessing a picture constitutes the crime of extreme pornography.

B *Teen pornography*

- i **It increases the likelihood of adolescent pregnancy:** Youth often exposed to sexually explicit content on television have a significantly increased risk of adolescent pregnancy (Chandra et al., 2008).
- ii **It is detrimental to sexual development:** When teenagers consume pornography, it can disorient them during a critical developmental stage when they need to learn how to manage their sexuality and are particularly vulnerable to questioning their sexual beliefs and moral principles (Peter and Valkenburg, 2008). Blocking access to adult material on internet-connected devices is a brilliant place to start when it comes to keeping pornography out of reach of teenagers.
- iii **It develops false expectations that obstruct average sexual growth:** Adolescents exposed to excessive pornography have reduced sexual self-esteem (Morrison et al., 2006). Maintaining a dialogue with kids about the impacts of pornography is critical for avoiding difficulties such as despair and low self-esteem.

- iv **It increases the chance of anxiety and depression:** There is also a substantial correlation between regular pornography usage and feelings of isolation, even profound despair, among adolescents (Ybarra and Mitchell, 2005; Yoder et al., 2005).

C *Child pornography*

Allison Baxter (2014) is of the view that child pornography leads to:

- i promoting aggression towards children
- ii normalising sexual harm
- iii adversely affecting healthy intimate relationships
- iv shaping negative attitudes as well as behaviours towards children
- v it could lead to addiction.

4 **Cyberstalking**

Cyberstalking The phrases ‘cyberstalking’ and ‘cyberbullying’ are sometimes synonymous. According to Marshall University (2021), cyberstalking is harassing or stalking another person through the internet or any telecommunication technology. It is more than the inconvenient nature of unwanted text or visuals. It is intentional, systematic, and relentless. The messages, whether from a known or unknown source, continue even after the receiver requests an end to all contact and are frequently laden with inappropriate and occasionally unsettling content.

However, cyberstalking is cyberbullying, which, along with ‘cybersquatting’ and ‘cyberterrorism’, is a rising range of computer- and internet-related crimes referred to collectively as cybercrime. While cyberstalking is a blanket word for online harassment, it may take various forms, including slander, defamation, false allegations, trolling, and even direct threats. It is a digital continuation of physical stalking (Awati, 2021).

According to Balaban (2018), Gordon (2021), and Kaspersky (2021), the respective tips are:

Avoiding cyberstalking

- i avoid disclosing sensitive information
- ii update the software
- iii maintain good digital hygiene
- iv hide the IP address
- v keep a low profile

If you are a victim of cyberstalking

- i block the individual
- ii please report it to the platform on which you are currently logged in
- iii contact the authorities.

To reduce damage

- i reduce the quantity of information about you that is publicly visible online
- ii increase the quantity of misleading info that an attacker may use to deceive you.

9 Discussion

The theory of planned behaviour (TPB) is a psycho-sociological theory that explains human behaviour by considering individual beliefs, attitudes, subjective norms, and perceived behavioural control. It provides a framework for understanding and predicting behaviours based on these psycho-sociological factors. When applied to “Multifaceted Issues of Cybercrime in the Contemporary Era,” the TPB can offer valuable insights into the factors influencing individuals’ engagement in cybercriminal activities or their susceptibility to becoming victims.

1 *Attitudes towards cybercrime*

TPB posits that attitudes toward a behaviour strongly influence one’s intention to perform that behaviour. Individuals may have various attitudes toward cybercrime, such as perceiving cybercriminal activities as financially rewarding, socially acceptable within certain groups, or even as a form of rebellion. Understanding these attitudes can provide insights into the motivations behind engaging in cybercrime.

2 *Subjective norms*

Subjective norms refer to perceived social pressure or approval/disapproval related to a behaviour. In the context of cybercrime, individuals may be influenced by the norms within their online communities or peer groups. If there is a perception that engaging in cybercriminal activities is socially acceptable or even encouraged within certain circles, individuals may be more inclined to participate.

3 *Perceived behavioural control*

This aspect of TPB focuses on an individual’s perception of their ability to perform a behaviour successfully. In the realm of cybercrime, perceived behavioural control might include factors such as technical skills, knowledge of hacking tools, and awareness of the legal consequences. Understanding how individuals perceive their control over cybercrime can shed light on their likelihood of participating in such activities.

4 *Intentions and actual behaviour*

According to TPB, intentions are a crucial predictor of actual behaviour. In the case of cybercrime, understanding the intentions behind engaging in such activities can help predict and prevent these behaviours. It could involve analysing factors such as the perceived benefits, motivations, and rationalisations that individuals may have for participating in cybercriminal activities.

5 *Prevention and intervention strategies*

Applying TPB to the multifaceted cybercrime issues can aid in developing targeted prevention and intervention strategies. By identifying and addressing the psychological factors influencing individuals’ intentions to engage in cybercrime, authorities, and

cybersecurity professionals can design more effective educational programs and legal and cybersecurity measures.

In summary, applying the TPB to “Multifaceted Issues of Cybercrime in the Contemporary Era” allows for a nuanced understanding of the psychological factors that drive individuals to participate in cybercriminal activities. This understanding can inform strategies for prevention, intervention, and the development of policies to address the complex challenges posed by cybercrime in the modern world.

1 Cyberterrorism and theory of planned behaviour

The TPB can be linked to ‘Cyberterrorism’ by providing insights into the psychological factors that influence individuals or groups to engage in cyberterrorist activities. Here is how TPB elements can be associated with the understanding of cyberterrorism:

i Attitudes toward cyberterrorism

TPB suggests that attitudes toward a behaviour significantly influence behavioural intentions. In cyberterrorism, individuals or groups may develop attitudes that justify or glorify cyberattacks for ideological, political, or religious reasons. Understanding these attitudes is crucial for predicting and preventing cyberterrorist acts.

ii Subjective norms in cyberterrorism

Subjective norms refer to perceived social pressure or approval/disapproval related to a behaviour. In the case of cyberterrorism, individuals or groups may be influenced by the norms within extremist online communities, where there might be approval for using cyber means to achieve political or ideological goals. Understanding these social influences is essential for devising strategies to counteract the spread of extremist ideologies.

iii Perceived behavioural control in cyberterrorism

Perceived behavioural control in TPB focuses on an individual’s perception of their ability to perform a behaviour successfully. In the context of cyberterrorism, this could involve technical capabilities, knowledge of cybersecurity measures, and awareness of potential countermeasures by authorities. Understanding the perceived control over engaging in cyberterrorist activities can help in developing effective strategies to mitigate these threats.

iv Intentions and actual behaviour in cyberterrorism

According to TPB, intentions are a crucial predictor of actual behaviour. In the case of cyberterrorism, understanding the intentions behind carrying out cyber attacks for terrorist purposes is essential for predicting and preventing such acts. Motivations, grievances, and ideological beliefs can shape these intentions.

v Prevention and counter-terrorism strategies

Applying TPB to cyberterrorism can inform the development of prevention and counter-terrorism strategies. By understanding the psychological factors contributing to the intention to engage in cyberterrorist activities, authorities, and cybersecurity professionals can design targeted interventions. It might include educational programs, community outreach efforts, and technological measures to detect and prevent cyberterrorist acts.

vi *Global collaboration and information sharing*

TPB can also highlight the importance of international collaboration in addressing cyberterrorism. Understanding the psychological factors on a global scale can facilitate information sharing among nations, enabling a more comprehensive and coordinated response to cyberterrorist threats.

2 **Cyber frauds and theory of planned behaviour**

The TPB can be linked to cyber fraud by providing insights into the psychological factors that influence individuals' intentions and behaviours related to fraudulent activities in the cyber realm. Here is how TPB elements can be associated with understanding cyber frauds:

i *Attitudes toward cyber frauds*

TPB suggests that individuals' attitudes toward a behaviour significantly influence their behavioural intentions. In the context of cyber fraud, individuals may develop attitudes influenced by perceived benefits, justifications, or rationalisations for engaging in fraudulent activities online. Understanding these attitudes is crucial for predicting and preventing cyber fraud incidents.

ii *Subjective norms in cyber frauds*

Subjective norms refer to perceived social pressure or approval/disapproval related to a behaviour. In the case of cyber fraud, individuals might be influenced by social norms within online communities that normalise or encourage fraudulent behaviours. It can include peer pressure, online forums, or criminal networks that support cyber fraud activities.

iii *Perceived behavioural control in cyber frauds*

Perceived behavioural control in TPB focuses on an individual's perception of their ability to perform a behaviour successfully. In the context of cyber fraud, this could involve technical skills, knowledge of cybersecurity vulnerabilities, and awareness of legal consequences. Understanding the perceived control over engaging in cyber fraud activities can inform prevention strategies and interventions.

iv *Intentions and actual behaviour in cyber frauds*

TPB posits that intentions are a crucial predictor of actual behaviour. In the case of cyber fraud, understanding the intentions behind engaging in fraudulent activities, such as financial motivations or personal gain, is essential for predicting and preventing such acts. Analysing these intentions helps in developing strategies to deter and detect cyber fraud.

v *Prevention and mitigation strategies*

Applying TPB to cyber fraud can inform the development of prevention and mitigation strategies. Cybersecurity professionals and law enforcement can design targeted interventions by understanding the psychological factors contributing to individuals' intentions to commit cyber fraud. It might involve education on cybersecurity best practices, awareness campaigns, and implementing technological measures to detect and prevent fraud.

vi *User education and awareness*

TPB highlights the importance of influencing attitudes and subjective norms. In the context of cyber fraud, this emphasises the need for user education and awareness programs to change attitudes towards engaging in fraudulent activities and to create a social environment that discourages such behaviours.

3 Pornography and theory of planned behaviour

The TPB can be linked to the topic of ‘Pornography’ by providing insights into the psychological factors that influence individuals’ attitudes, intentions, and behaviours related to the consumption or production of pornography. Here is how TPB elements can be associated with understanding the dynamics surrounding pornography:

i *Attitudes toward pornography*

TPB suggests that attitudes significantly influence behavioural intentions. In the context of pornography, individuals may have varying attitudes, such as perceiving it as a form of entertainment, self-expression, or even as a controversial and potentially harmful activity. Understanding these attitudes is essential for predicting and comprehending the factors that influence the consumption or production of pornography.

ii *Subjective norms concerning pornography*

Subjective norms refer to perceived social pressure or approval/disapproval related to a behaviour. Regarding pornography, individuals might be influenced by societal norms, cultural values, and peer attitudes. Social perceptions of whether pornography is accepted or stigmatised can shape individuals’ decisions and behaviours in this domain.

iii *Perceived behavioural control regarding pornography*

Perceived behavioural control in TPB focuses on an individual’s perception of their ability to perform a behaviour successfully. In the context of pornography, this could include factors such as access to materials, legal considerations, and personal values regarding self-control. Understanding perceived behavioural control can inform interventions promoting responsible and ethical consumption.

iv *Intentions and actual behaviour concerning pornography*

TPB posits that intentions are a crucial predictor of actual behaviour. Regarding pornography, understanding individuals’ intentions – whether it is for personal gratification, curiosity, or other reasons – provides insights into the factors that drive consumption or production. Analysing intentions is crucial for developing strategies that address potential negative consequences or promote responsible use.

v *Public health and education campaigns*

Applying TPB to the topic of pornography can inform public health and education campaigns. By understanding the psychological factors that contribute to individuals’ intentions and behaviours, educational initiatives can be designed to promote healthy attitudes, consent, and awareness of potential risks associated with consuming or producing explicit content.

vi Legal and ethical considerations

TPB can highlight the role of legal and ethical considerations in the context of pornography. Understanding perceived behavioural control includes assessing individuals' awareness of legal regulations, ethical boundaries, and potential harm associated with certain types of explicit content. This understanding can guide legal frameworks and educational efforts to promote responsible behaviour.

4 Cyberstalking and the theory of planned behaviour

The TPB can be linked to 'Cyberstalking' by offering insights into the psychological factors that influence individuals' attitudes, intentions, and behaviours related to cyberstalking. Here is how TPB elements can be associated with understanding the dynamics of cyberstalking:

i Attitudes toward cyberstalking

TPB emphasises that attitudes significantly influence behavioural intentions. In cyberstalking, individuals may have attitudes shaped by various factors, such as a perceived sense of control, revenge, or the desire for power and intimidation. Understanding these attitudes is crucial for predicting and preventing cyberstalking incidents.

ii Subjective norms in cyberstalking

Subjective norms refer to perceived social pressure or approval/disapproval related to a behaviour. Individuals engaging in cyberstalking might be influenced by social norms within specific online communities or peer groups that condone or encourage such behaviour. Understanding these subjective norms can inform efforts to change social perceptions and discourage cyberstalking.

iii Perceived behavioural control in cyberstalking

Perceived behavioural control in TPB focuses on an individual's perception of their ability to perform a behaviour successfully. In the context of cyberstalking, this could include technical skills, anonymity, and the perception of avoiding legal consequences. Understanding perceived behavioural control is essential for developing prevention and intervention strategies.

iv Intentions and actual behaviour in cyberstalking

TPB posits that intentions are a crucial predictor of actual behaviour. In the case of cyberstalking, understanding the intentions behind engaging in such behaviour – whether driven by obsession, revenge, or harassment – is crucial for predicting and preventing cyberstalking incidents. Analysing these intentions helps in developing strategies to deter and address cyberstalking effectively.

v Prevention and intervention strategies

Applying TPB to cyberstalking can inform the development of prevention and intervention strategies. Law enforcement and cybersecurity professionals can design targeted interventions by understanding the psychological factors contributing to individuals' intentions to engage in cyberstalking. It might involve educational programs, awareness campaigns, and legal measures to address and prevent cyberstalking.

vi *Technological countermeasures*

TPB can also guide the development of technological countermeasures to prevent and combat cyberstalking. Understanding perceived behavioural control includes assessing individuals' knowledge of the technological tools and methods used in cyberstalking. Enhancing cybersecurity measures and educating users about protecting their online presence can be essential to addressing cyberstalking.

10 Research limitations

Limitations of the study on the multifaceted issues of cybercrime in the contemporary era may include, but are not limited to:

- 1 **Sample size:** The study may have limitations if the sample size is too small or the participants are not representative of the population under study.
- 2 **Data availability:** Due to the sensitive nature of cybercrime, obtaining relevant data may be challenging, limiting the study's depth.
- 3 **Constraints:** The complexity and constantly evolving nature of cybercrime may limit the time to complete a comprehensive study.
- 4 **Bias:** The study may be biased if the researcher has preconceived ideas or biases that influence the interpretation of data.
- 5 **Research design:** The study may have limitations if the research design used is not appropriate for the research question under study.
- 6 **Context:** The study's findings may be limited to the specific context in which the research is challenging to generalise the results to other settings.
- 7 **Data quality:** The study's conclusions may be limited by the quality of the data collected, such as incomplete or inaccurate data.

11 Conclusion

Cybercrime research is in its infancy, as the area is relatively young. The internet is one of today's intriguing revolutionary innovations since it continues to transform the daily lives of billions across the globe. Because technological advancements invariably result in the evolution of cybercrime, some tend to view cybercrime as an ever-changing collection of behaviours. The most pervasive and detrimental issues encompassing the digital era are cyberterrorism, cyber fraud, pornography, and cyberstalking. Cybercrime, the offspring of contemporary technology, could only be controlled and prevented by employing robust, strong cyber legislation and concrete initiatives. Nations worldwide face cybercrime for numerous reasons, e.g., inadequate technology, absence, the incapacity of legislation regarding financial constraints, and lack of cooperation with international law enforcement agencies.

12 Recommendations

- 1 Expert perspectives from psychologists, sociologists, criminologists, and information technology specialists should be incorporated into cybercrime law.
- 2 Programs to educate the general population about cybercrime should be launched. It can be done by engaging the community and CBOs, NGOs, INGOs, and cyber vigilantism.
- 3 A solid global cyber army capable of countering cyber attacks is necessary.
- 4 Students must be encouraged to learn about the risks of the digital environment through workshops and lectures.
- 5 At the domestic level, a special task force (i.e., cyber police) should be developed to ensure routine online checks at public internet access facilities.
- 6 Experts must explore cybercrime concerns in various venues, including electronic and print media.
- 7 Respective countries should maintain proper cybercrime data, and it should be shared.
- 8 Cybercrime victims are numerous, and victims should have simple access to a complaint mechanism for e-offenses.
- 9 Courses on the cyber world should be integrated into information technology, social science, business, and law studies.
- 10 The appropriate courts (especially in undeveloped countries) should be adequately trained to prosecute cyber charges.
- 11 Legal departments must be provided with cutting-edge investigative technology.

13 Additional recommendations (For individuals)

- 12 Utilise privacy controls on social media sites to limit the public dissemination of private details.
- 13 Use your computer and terminate online sessions altogether.
- 14 Use security programs, protect your passwords, and visit only trustworthy websites.
- 15 Encryption of files and regular backups of necessary data is essential.
- 16 Never click on links sent to you by strangers.
- 17 Limiting the administrative powers of all accounts in case of shared devices.
- 18 After logging out of an account, delete all history and keep the updated software package.
- 19 Wi-Fi networks and Bluetooth connections should be avoided.
- 20 E-transactions must be entered via authentic websites, and data should not be saved on online servers.

14 Research implications

- 1 **Policy and legislative development:** Research on the multifaceted cybercrime issues can provide valuable insights for policymakers and legislators. The findings can inform the development of comprehensive and up-to-date policies and legislation to address the evolving nature of cyber threats. It can contribute to formulating effective cybercrime prevention strategies, data protection regulations, and legal frameworks that promote cybersecurity and deter cybercriminals' activities.
- 2 **Cybersecurity education and awareness:** The research can affect cybersecurity education and awareness programs. Understanding the multifaceted cybercrime issues can help identify the knowledge and skills needed to protect individuals and organisations from cyber threats. The research findings can guide the development of educational curricula, training programs, and public awareness campaigns that enhance cybersecurity literacy and promote responsible online behaviour.
- 3 **Industry practices and standards:** Research on the multifaceted cybercrime issues can influence industry practices and standards. It can highlight the vulnerabilities, emerging threats, and best cybersecurity practices. The findings can contribute to developing industry-specific guidelines, cybersecurity frameworks, and standards that promote safe practices, risk management, and resilience against cyber attacks.
- 4 **International collaboration and cooperation:** The research can have implications for international collaboration and cooperation in combating cybercrime. By understanding the multifaceted issues and challenges, researchers can identify areas where international cooperation is essential, such as information sharing, joint investigations, and capacity-building initiatives. The findings can guide efforts to enhance collaboration among nations, promote harmonisation of cybercrime laws, and develop frameworks for international response to cyber threats.
- 5 **Technological innovations:** The multifaceted issues of cybercrime can stimulate technological innovations and advancements in cybersecurity. The research can highlight areas where technology can be crucial in preventing, detecting, and mitigating cyber threats. It can inspire the development of new cybersecurity tools, techniques, and solutions that address cybercriminals' evolving tactics and techniques.
- 6 **Public-private partnerships:** Research on the multifaceted cybercrime issues can encourage public-private partnerships in cybersecurity. The findings emphasise the importance of collaboration between government entities, private sector organisations, and academic institutions in addressing cyber threats. It can foster dialogue, information sharing, and joint initiatives to enhance cybersecurity capabilities, develop innovative solutions, and promote a coordinated response to cybercrime.
- 7 **International norms and cyber diplomacy:** The research can contribute to the establishment of international norms and practices in cyberspace. By understanding the multifaceted issues of cybercrime, researchers can identify areas where norms and rules can be developed to promote responsible state behaviour and deter cybercriminals' activities. The findings can inform cyber diplomacy efforts, negotiations, and discussions to establish a secure and stable cyberspace.

- 8 **Social and economic impact:** Research on the multifaceted issues of cybercrime can provide insights into cyber threats' social and economic impact. It can inform policymakers and stakeholders about the potential consequences of cybercrime on individuals, businesses, and societies. The findings can guide the allocation of resources, investment in cybersecurity measures, and development of support systems for victims of cybercrime.

Considering these research implications, stakeholders can leverage the findings to strengthen cybersecurity practices, inform policy decisions, foster collaboration, and promote a secure and resilient digital environment. The research can contribute to mitigating the risks and challenges of cybercrime, protecting individuals and organisations, and maintaining trust and confidence in the digital era.

15 Future research directions

Crucial avenues for undertaking future studies involving cybercrime by engaging quantitative, qualitative, or mixed techniques could be:

- 1 criminal psychology
- 2 cyberterrorism
- 3 cybersecurity
- 4 perceived and actual risks in cybercrime.

References

- Abaimov, S. and Martellini, M. (2020) *Cyber Arms Security in Cyberspace*, CRC Press, Boca Raton, Florida, USA.
- Apau, R. and Koranteng, F.N. (2019) 'Impact of cybercrime and trust on the use of e-commerce technologies: an application of the theory of planned behavior', *International Journal of Cyber Criminology*, Vol. 13, No. 2, pp.228–254.
- Austin, G. (2020) *National Cyber Emergencies: The Return to Civil Defense*, Routledge, London, UK.
- Awati, R. (2021) *Cyberstalking*, August, <https://www.techtarget.com/searchsecurity/definition/cyberstalking>
- Azevedo, F.U.B. (2018) *Hackers Exposed: Discover the Secret World of Cybercrime*, Independently Published.
- Balaban, D. (2018) 'What cyberstalking is and how to prevent it', *The State of Security*, 5 December, <https://www.tripwire.com/state-of-security/theim/security-awareness/what-cyberstalking-prevent/>
- Bancroft, A. (2019) *The Darknet and Smarter Crime: Methods for Investigating Criminal Entrepreneurs and the Illicit Drug Economy (Palgrave Studies in Cybercrime and Cybersecurity)*, Palgrave Macmillan, London, UK.
- Bandler, J. and Merzon, A. (2020) *Cybercrime Investigations: A Comprehensive Resource for Everyone*, CRC Press, Boca Raton, Florida, USA.
- Baxter, A. (2014) 'How pornography harms children: the advocate's role', *American Bar Association*, 1 May, https://www.Americanbar.org/groups/public_interest/child_law/resources/child_law_practice_online/child_law_practice/vol-33/may-2014/how-pornography-harms-children--the-advocate-s-role/

- Benson, V. and McAlaney, J. (2019) *Emerging Cyber Threats and Cognitive Vulnerabilities*, 1st ed., Academic Press, Cambridge, Massachusetts, USA.
- Brand, M., Snagowski, J., Laier, C. and Maderwald, S. (2016) 'Ventral striatum activity when watching preferred pornographic pictures is correlated with symptoms of internet pornography addiction', *NeuroImage*, Vol. 129, pp.224–232, doi: 10.1016/j.neuroimage. 2016.01.033.
- Brand, M., Young, K.S. and Laier, C. (2014) 'Prefrontal control and internet addiction: a theoretical model and review of neuropsychological and neuroimaging findings', *Frontiers in Human Neuroscience*, Vol. 8, p.375, doi: 10.3389/fnhum. 2014.00375.
- Bridges, A.J. and Morokoff, P.J. (2011) 'Sexual media use and relational satisfaction in heterosexual couples', *Personal Relationship*, Vol. 18, pp.562–585, doi: 10.1111/j.1475-6811. 2010.01328.x.
- Carlson, C.T. (2019) *How to Manage Cybersecurity Risk: A Security Leader's Roadmap with an Open Fair*, Universal Publishers, Irvine, California, USA.
- Chandra, A., Martino, S.C., Collins, R.L., Elliott, M.N., Berry, S.H., Kanouse, D.E. and Miu, A. (2008) 'Does watching sex on television predict teen pregnancy? findings from a longitudinal survey of youth', *Pediatrics*, Vol. 122, pp.1047–1054.
- Cripps, D. (2021) 'Tackling the cybercrime pandemic in 2021', *Security Magazine*, 21 September, <https://www.securitymagazine.com/articles/96134-tackling-the-cybercrime-pandemic-in-2021>
- Cybercrime (2021a) *Encyclopedia Britannica*, <https://www.britannica.com/topic/cybercrime>
- Cybercrime (2021b) *Collins English Dictionary*, <https://www.collinsdictionary.com/dictionary/english/cybercrime>
- Cybercrime (2021c) *The Chambers Dictionary*, <https://www.cybercrimechambers.com/blog-web-jacking-117.php>
- Cybercrime (2021d) *Merriam-Webster*, <https://www.merriam-webster.com/dictionary/cybercrime>
- Cybercrime (2021e) *Oxford Advanced Learner's Dictionary*, <https://www.oxfordlearnersdictionaries.com/definition/english/cybercrime>
- Duffy, A., Dawson, D.L. and das Nair, R. (2016) 'Pornography addiction in adults: a systematic review of definitions and reported impact', *Journal of Sexual Medicine*, Vol. 13, pp.760–777, doi: 10.1016/j.jsxm.2016.03.002.
- Dwulit, A.D. and Rzymiski, P. (2019) 'Prevalence, patterns and self-perceived effects of pornography consumption in polish university students: a cross-sectional study', *International Journal of Environmental Research and Public Health*, Vol. 16, No. 10, p.1861, doi: 10.3390/ijerph16101861.
- Edwards, B.P. (2019) *Cybersecurity Oversight Liability*, Scholarly Works, <https://scholars.law.unlv.edu/facpub/1220>
- EmBroker (2021) *2021 Must-Know Cyber Attack Statistics and Trends*, 11 August, <https://www.embroker.com/blog/cyber-attack-statistics/>
- Fink, A. (2019) *Conducting Research Literature Reviews: From the Internet to Paper*, SAGE Publications, Thousand Oaks, California, USA.
- Gillespie, A.A. (2019) *Cybercrime: Key Issues and Debates*, Routledge, London, UK.
- Glenny, M. (2012) *DarkMarket: How Hackers Became the New Media*, Vintage Books, New York, USA.
- Goodwin, B.C., Browne, M. and Rockloff, M. (2015) 'Measuring preference for super-normal over natural rewards: a two-dimensional anticipatory pleasure scale', *Evolutionary Psychology*, Vol. 5, p.13, doi: 10.1177/1474704915613914.
- Gordon, S. (2021) *What is Cyberstalking?*, 16 August, <https://www.verywellmind.com/what-is-cyberstalking-5181466>
- Graham, R.S. and Smith, S.K. (2019) *Cybercrime and Digital Deviance*, 1st ed., Routledge, London, UK.

- Grubbs, J.B. and Gola, M. (2019) 'Is pornography use related to erectile functioning? results from cross-sectional and latent growth curve analyses', *Journal of Sexual Medicine*, Vol. 16, pp.111–125, doi: 10.1016/j.jsxm.2018.11.004.
- Grubbs, J.B. and Perry, S.L. (2019) 'Moral incongruence and pornography use: a critical review and integration', *Journal of Sex Research*, Vol. 56, pp.29–37, doi: 10.1080/00224499.2018.1427204.
- Harris, D. (2019) *Literature Review and Research Design: A Guide to Effective Research Practice*, Routledge, London, UK.
- Hempel, S. (2019) *Conducting your Literature Review*, American Psychological Association, Washington, DC, USA.
- Hilton Jr., D.L. (2013) 'Pornography addiction—a supra-normal stimulus considered in the context of neuroplasticity', *Socioaffective Neuroscience and Psychology*, Vol. 3, p.20767, doi: 10.3402/snp.v3i0.20767.
- Hudak, H.C. (2019) *Cybercrime (Privacy in the Digital Age)*, North Star Editions.
- Hufnagel, S. and Moiseienko, A. (2019) *Criminal Networks and Law Enforcement: Global Perspectives on the Illegal Enterprise*, Routledge, London, UK.
- Hutchings, A. (2013) *Theory and Crime: Does It Compute?*, Griffith University, Brisbane, Queensland, Australia.
- Jafarkarimi, H., Saadatdoost, R., Sim, A.T.H. and Hee, J.M. (2016) 'Behavioral intention in social networking sites ethical dilemmas: an extended model based on the theory of planned behavior', *Computers in Human Behavior*, Vol. 62, pp.545–561.
- Johansen, G. (2020) *Digital Forensics and Incident Response: Incident Response Techniques and Procedures to Respond to Modern Cyber Threats*, Packt Publishing, Birmingham.
- Jones, C.W. (2005) 'Council of Europe convention on cybercrime: themes and critiques', *Workshop on the International Dimensions of Cybersecurity*, Hosted by Georgia Institute of Technology and Carnegie Mellon University, USA, April.
- Kaspersky (2021) *Tips to Protect Yourself from Cyberstalkers*, <https://www.kaspersky.com/resource-center/threats/how-to-avoid-cyberstalking>
- Kim, P. (2018) *The Hacker Playbook 3: Practical Guide to Penetration Testing*, Independently Published.
- Klucken, T., Wehrum-Osinsky, S., Schweckendiek, J., Kruse, O. and Stark, R. (2016) 'Altered appetitive conditioning and neural connectivity in subjects with compulsive sexual behavior', *Journal of Sexual Medicine*, Vol. 3, pp.627–636, doi: 10.1016/j.jsxm.2016.01.013.
- Komba, M.M. and Lwoga, E.T. (2020) *Systematic Review as a Research Method in the Library and Information Science*, doi: 10.4018/978-1-7998-1471-9.ch005.
- Koukounas, E. and Over, R. (1997) 'Male sexual arousal elicited by film and fantasy matched in content', *Australian Journal of Psychology*, Vol. 49, pp.1–5, doi: 10.1080/00049539708259843.
- Kuhn, S. and Gallinat, J. (2014) 'Brain structure and functional connectivity associated with pornography consumption: the brain on porn', *JAMA Psychiatry*, Vol. 71, pp.827–834, doi: 10.1001/jamapsychiatry.2014.93.
- Laan, E. and Everaerd, W. (1995) 'Habituation of female sexual arousal to slides and film', *Archives of Sexual Behavior*, Vol. 24, pp.517–541, doi: 10.1007/BF01541832.
- LaMorte, W.W. (2019) *The Theory of Planned Behavior*, Boston University School of Public Health, 9 September, <https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchange/theories/BehavioralChangeTheories3.html>
- Lavorgna, A. (2020) *Cybercrimes: Critical Issues in a Global Context*, Springer, New York, USA.
- Leukfeldt, R. and Holt, T.J. (2019) *The Human Factor of Cybercrime*, Routledge, London, UK.
- Ley, D., Prause, N. and Finn, P. (2014) 'The emperor has no clothes: a review of the "Pornography Addiction Model"', *Current Sexual Health Reports*, Vol. 6, pp.94–105, doi: 10.1007/s11930-014-0016-8.

- Littler, M. and Lee, B. (2020) *Digital Extremisms: Readings in Violence, Radicalization, and Extremism in the Online Space*, Springer Nature Switzerland A.G.
- Love, T., Laier, C., Brand M., Hatch, L. and Hajela, R. (2015) 'Neuroscience of internet pornography: a review and update', *Behavioral Science*, Vol. 5, pp.388–433, doi: 10.3390/bs5030388.
- Lusthaus, J. (2012) 'Trust in the world of cybercrime', *Global Crime*, Vol. 13, No. 2, pp.71–94.
- Marion, N.E. and Twede, J. (2020) *Cybercrime: An Encyclopedia of Digital Crime*, ABC-CLIO.
- Marsh, B. and Melville, G. (2019) *Crime, Justice, and the Media*, Routledge, London, UK.
- Marshall University (2021) *Cyberstalking*, <https://www.marshall.edu/wcenter/stalking/cyberstalking/>
- Martellozzo, E. and Jane, E.A. (2017) *Cybercrime and Its Victims*, Routledge, London, UK.
- McQuade, S.C. (Ed.) (2008) *Encyclopedia of Cybercrime*, ABC-CLIO.
- Morrison, T.G., Ellis, S.R., Morrison, M.A., Bearden, A. and Harriman, R.L. (2006) 'Exposure to sexually explicit material and variations in body esteem, genital attitudes, and sexual esteem among a sample of Canadian men', *The Journal of Men's Studies*, Vol. 14, pp.209–222.
- Nair, A. (2018) *The Regulation of Internet Pornography: Issues and Challenges*, Routledge, London, UK, doi: 10.1152/ajplung.00544.2017.
- Packetlabs (2021) *Cybersecurity Statistics for 2021*, 3 August, <https://www.packetlabs.net/cybersecurity-statistics-2021/>
- Park, B.Y., Wilson, G., Berger, J., Christman, M., Reina, B., Bishop, F., Klam, W.P. and Doan, A.P. (2016) 'Is internet pornography causing sexual dysfunctions? A review with clinical reports', *Behavioral Science*, Vol. 6, p.17, doi: 10.3390/bs6030017.
- Pawson, R., Greenhalgh, T., Harvey, G. and Walshe, K. (2005) 'Realist review – A new method of systematic review designed for complex policy interventions', *Journal of Health Services Research and Policy*, Vol. 10, No. 1, pp.21–34.
- Perry, S.L. (2016) 'Does viewing pornography reduce marital quality over time? Evidence from longitudinal data', *Archives of Sexual Behavior*, Vol. 46, pp.549–559, doi: 10.1007/s10508-016-0770-y.
- Peter, J. and Valkenburg, P.M. (2008) 'Adolescents' exposure to sexually explicit internet material, sexual uncertainty, and attitudes toward uncommitted sexual exploration: Is there a link?', *Communication Research*, Vol. 35, pp.579–601.
- Petticrew, M. and Roberts, H. (2006) *Systematic Reviews in the Social Sciences: A Practical Guide*, doi: 10.1002/9780470754887.
- Ponemon Institute (2018) *State of Endpoint Security Risk*, <https://www.businesswire.com/news/home/20181016005758/en/Study-Reveals64-Organizations-Experienced-Successful-Endpoint>
- Poulsen, F.O., Busby, D.M. and Galovan, A.M. (2013) 'Pornography use: who uses it and how it is associated with couple outcomes', *Journal of Sex Research*, Vol. 50, pp.72–83, doi: 10.1080/00224499.2011.648027.
- PurpleSec (2021) *Cybercrime Up 600% Due to COVID-19 Pandemic*, <https://purplesec.us/resources/cyber-security-statistics/>
- Purssell, E. and McCrae, N. (2020) *How to Perform a Systematic Literature Review: A Guide for Healthcare Researchers, Practitioners and Students*, Springer International Publishing, New York, USA.
- Rahi, S. (2017) 'Research design and methods: a systematic review of research paradigms, sampling issues, and instruments development', *International Journal of Economics and Management Sciences*, No. 6, pp.1–5, doi: 10.4172/2162-6359.1000403.
- Sangster, M. (2020) *No Safe Harbor: The Inside Truth about Cybercrime-and How to Protect your Business*, Page Two.
- Schober, S.N. and Schober, C.W. (2019) *Cybersecurity is Everybody's Business: Solve the Security Puzzle for your Small Business and Home*, ScottSchober.com Publishing, Metuchen, New Jersey, USA.

- Smith (2018) *Hacking Pacemakers, Insulin Pumps, and Patient's Vital Signs in Real-Time*, <https://www.csoonline.com/article/3296633/security/hacking-pacemakers-insulin-pumps-an-d-patients-vital-signs-in-real-time.html>
- Sniewski, L., Farvid, P. and Carter, P. (2018) 'The assessment and treatment of adult heterosexual men with self-perceived problematic pornography use: a review', *Addictive Behaviors*, Vol. 77, pp.217–224, doi: 10.1016/j.addbeh.2017.10.010.
- Steele, V.R., Staley, C., Fong, T. and Prause, N. (2013) 'Sexual desire, not hypersexuality, is related to neurophysiological responses elicited by sexual images', *Socioaffective Neuroscience and Psychology*, Vol. 3, p.20770, doi: 10.3402/snp.v3i0.20770.
- Steinberg, J. (2019) *Cybersecurity for Dummies (For Dummies Computer/Tech)*, John Wiley & Sons, Hoboken, New Jersey, USA.
- Sun, C., Bridges, A., Johnason, J. and Ezzell, M. (2014) 'Pornography and the male sexual script: an analysis of consumption and sexual relations', *Archives of Sexual Behavior*, Vol. 45, p.995, doi: 10.1007/s10508-016-0744-0.
- The Daily Swig (2021) *Latest Cybercrime News*, <https://portswigger.net/daily-swig/cybercrime>
- Troia, V. (2020) *Hunting Cybercriminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques*, Indianapolis, Wiley, Hoboken, New Jersey.
- Victor, L. (2008) 'Systematic reviewing in the social sciences: outcomes and explanation', *Enquire*, Vol. 1, No. 1, pp.32–46.
- Wery, A. and Billieux, J. (2016) 'Online sexual activities: an exploratory study of problematic and non-problematic usage patterns in a sample of men', *Computers in Human Behavior*, Vol. 56, pp.257–266, doi: 10.1016/j.chb.2015.11.046.
- Wilkinson, E. (2017) 'The diverse economies of online pornography: from paranoid readings to post-capitalist futures', *Sexualities*, Vol. 20, pp.981–998, doi: 10.1177/1363460716675141.
- Willems, E. (2019) *Cyber Danger: Understanding and Guarding Against Cybercrime*, Springer International Publishing, New York, USA.
- Wright, P.J., Sun, C. and Steffen, N. (2018) 'Pornography consumption, perceptions of pornography as sexual information, and condom use', *Journal of Sex and Marital Therapy*, Vol. 10, pp.1–6, doi: 10.1080/0092623X.2018.1462278.
- Yar, M. and Steinmetz, K.F. (2019) *Cybercrime and Society*, 3rd ed., SAGE Publications Ltd., Thousand Oaks, California, USA.
- Ybarra, M.L. and Mitchell, K.J. (2005) 'Exposure to internet pornography among children and adolescents: a national survey', *Cyber Psychology and Behavior*, Vol. 8, pp.473–486.
- Yoder, V.C., Virden, T.B. and Amin, K. (2005) 'Internet pornography and loneliness: an association?', *Sexual Addiction and Compulsivity*, Vol. 12, pp.19–44.
- Zhang, J. and Jemmott, J.B. (2015) 'Unintentional exposure to online sexual content and sexual behavior intentions among college students in China', *Asia-Pacific Journal of Public Health*, Vol. 27, pp.561–571, doi: 10.1177/1010539514562446.
- Zillmann, D. and Bryant, J. (2006) 'Pornography's impact on sexual satisfaction', *Journal of Applied Social Psychology*, Vol. 18, pp.438–453, doi: 10.1111/j.1559-1816.1988.tb00027.x.

Bibliography

- Beaver, K. (2017) *Hacking for Dummies*, 5th ed., For Dummies.
- Martens, M., De Wolf, R. and De Marez, L. (2019) 'Investigating and comparing the predictors of the intention towards taking security measures against malware, scams, and cybercrime in general', *Computers in Human Behavior*, Vol. 92, pp.139–150.
- Milkovich, D. (2018) *13 Alarming Cybersecurity Facts and Stats*, 3 December, <https://www.cybintsolutions.com/cyber-security-facts-stats/>

- Nohe, P. (2018) *Re-Hashed: 2018 Cybercrime Statistics: A Closer Look at the Web of Profit*, 27 September, <https://www.thesslstore.com/blog/2018-cybercrime-statistics/>
- Summo3000 (2018) *Top 20 Countries Found to Have the Most Cybercrime*, <https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/>
- Synodinou, T.E., Jogleux, P., Markou, C. and Prastitou-Merdi, T. (Eds.) (2020) *EU Internet Law in the Digital Era – Regulation and Enforcement*, Springer International Publishing, New York, USA, doi: 10.1007/978-3-030-25579-4.
- Webber, C. (2014) *Hackers and Cybercrime, A Primer on Crime, Deviance, and Social Harm*, Routledge, London, UK.
- White, R. (2018) *Saving Women From Sex Trafficking*, 13 November, <https://www.commercialappeal.com/story/opinion/contributors/2018/11/13/saving-women-sex-trafficking-opinion/1993547002/>
- Yar, M. (2013) *Cybercrime and Society*, Sage Publishing Ltd., Thousand Oaks, California, USA.
- Zhang, X., Tsang, A., Yue, W.T. and Chau, M. (2015) ‘The classification of hackers by knowledge exchange behaviors’, *Information Systems Frontiers*, Vol. 7, No. 6, pp.1239–1251.