A systematic literature review on cyberstalking. An analysis of past achievements and future promises

Puneet Kaur a, b, Amandeep Dhir b, c, d, *, Anushree Tandon e, Ebtesam A. Alzeiby g, Abeer Ahmed Abohassan f

a Department of Psychosocial Science, University of Bergen, Norway
b Openia Research Focus Area, North-West University, Vanderbijlpark, South Africa
c Department of Management, School of Business & Law, University of Agder, Kristiansand, Norway
d The Norwegian School of Hotel Management, Faculty of Social Sciences, Stavanger, Norway
e Turk School of Economics, University of Turku, Finland
f Social Planning Department, College of Social work, Princess Nourah bint Abdulrahman University
g Psychology Department, College of Education, Princess Nourah bint Abdulrahman University

ARTICLE INFO
Keywords:
Cyberstalking
Systematic literature review
thematic analysis
victimization
technology use

ABSTRACT
Individuals’ excessive use of technology-enabled communication platforms, such as social media, has led to scholarly recognition of rising incidences of cyberstalking. Despite considerable studies directed at its examination, the current research on cyberstalking is limited by a lack of clarity on its characterization and prevalence, coupled with a fragmented research focus. To address this limitation, a Systematic Literature Review (SLR) on cyberstalking has been undertaken. Rigorous protocols were applied to identify 49 empirical studies via Scopus and Web of Science, based on specific keywords and article selection criteria. Findings reveal four emergent research themes on characteristics and roles of cyberstalkers, victims, parents, social media, and online service providers, as well as reporting, coping, and prevention strategies discussed in prior studies. Findings imply the need for temporal and cross-cultural validation of measurement scales and prior results by developing sophisticated, theoretically-grounded frameworks. Based on study findings, a research framework is proposed to assist researchers in future examinations of under-investigated associations and constructs. Implications arise for studying potential pre-emptive factors to address cyberstalking at a societal level by disseminating appropriate information to the general public. There is a need to develop stringent legislation and to induce service providers’ active participation to prevent cyberstalking.

1. Introduction

The prolific growth of technology has engendered a plethora of next-generation media and communications platforms (e.g., Instagram, Facebook, Snapchat) that enable higher degrees of technology-supported interactions between individuals across the globe. With over 4 billion users of the Internet, and an estimated 3.4 billion active users of social media in 2019 (Statista, 2019, p. 8), the ubiquitous use of these platforms has been acknowledged to result in several positive implications for users, such as accumulating social capital (Benson et al., 2019), navigating new and diversified academic environments (Alt, 2017) and overseas locations (Hetz et al., 2015), as well as engaging in open learning (Al-Rahmi et al., 2019). However, scholars also acknowledge that a negative or dark side is associated with the excessive use of such Internet and social media platforms: fake news sharing (Talwar et al., 2019; Talwar et al., 2020), cyberbullying (Al-Rahmi et al., 2019), trolling (Salo et al., 2018), problematic sleep (Evers et al., 2020; Tandon et al., 2020) and fear of missing out (Blachnio and Przepiórka, 2018).

The academic community has demonstrated increasing interest in the study of these dark aspects of the Internet and social media use as well as functionality (Fox and Moreland, 2015), among which is the phenomenon of cyberstalking (Baccarella et al., 2018). Cyberstalking is understood as repetitive and unwanted communication or contact that is
directed toward an individual through electronic means (e.g., Internet, social media, email or other forms of technology) (Maple et al., 2012; Marcum et al., 2017; Noble et al., 2014; Paufl et al., 2009; Strawhun et al., 2013). An aspect of cyber-victimization (Lohbeck and Petermann, 2018), cyberstalking is posited to evoke negative emotions such as fear, distress, concern, or helplessness (Al-Rahimi et al., 2019; Maple et al., 2012; Noble et al., 2014).

Numerous studies have been conducted recently to study different issues related to cyberstalking, including victimization risk (Welsh and Lavoie, 2012), demographic characteristics (Lohbeck and Petermann, 2018; Reyns et al., 2018) including victim profiles (Pereira and Matos, 2016), stalker characteristics (Ménard and Pincus, 2012; Pereira and Matos, 2016; Smoker and March 2017), as well as victim-offender relationship (Dreiling et al., Bailler et al., 2014; Short et al., 2015). Additionally, previous literature has focused on identifying the motivational correlations (Dreiling et al., 2014), impacts of personality traits (Smoker and March 2017), and consequences of cyberstalking, such as adverse effects on mental health (Morris et al., 2019), use of coping strategies (Begotti and Maran, 2019) as well as management tactics (Tokunaga and Aune, 2017), and patterns in reporting the offenses (Fissel, 2018).

Despite the increasing number of studies focused on cyberstalking over the past decade, there have been limited attempts to devise a holistic and comprehensive understanding of cyberstalking from an academic perspective (e.g., Abghrim and Terrance, 2018; Pereira and Matos, 2016; Reynolds, 2019; Reynolds et al., 2018). The extant literature has also acknowledged a dearth of studies aimed at strengthening conceptual foundations of cyberstalking through strong theoretical grounding and rigorous empirical testing (Reyns et al., 2018). This indicates a need to re-examine cyberstalking and literature on this phenomenon in order to bring scholarly attention to emergent issues that have been under-investigated and/or require further validation. To address this need, the current study aims to undertake a systematic literature review (SLR) of empirical investigations of cyberstalking in the past decade with the specific objective of summarizing past research and delineating agendas for advancing research in this field.

The present SLR aims to answer four specific research questions (RQs). These are:

**RQ1.** What is the present status and profile of extant research on cyberstalking?

**RQ2.** What are the major thematic areas that have received attention from the academic community to date?

**RQ3.** What gaps and limitations in prior literature must be addressed?

**RQ4.** What are the future research directions that may be taken to advance existing research and literature on cyberstalking?

To answer these specific queries, the present study involves review and summarization of 49 studies identified in two comprehensive online databases, following a stringent protocol adapted from prior studies (e.g., Behera et al., 2019). A state-of-the-art research profile, emergent research themes, and limitations detailed in previous studies are presented based on current study findings. Insights gained through this SLR were also utilized to delineate gaps in current knowledge and to suggest future agendas for the advancement of research on cyberstalking. Further, a research framework has been developed to assist scholars’ future efforts by explicating specific variables, associations, key topics, and open issues that should be examined to develop a more nuanced conceptual and operational understanding of cyberstalking.

The manuscript is structured in five sections. Section two provides a brief overview of the topic being investigated (i.e., cyberstalking), and section three discusses methods and protocols followed for executing this SLR, along with a state-of-the-art research profile of reviewed studies. Section four presents the primary research themes derived from this review. Section five discusses the gaps and limitations identified, along with emerging directions for future research. A synthesized research framework is also presented in section five to assist scholars in advancing cyberstalking research. Section six consists of concluding remarks, including on the implications and limitations of this study.

## 2. Cyberstalking

Compared to other phenomena associated with the dark side of the Internet and social media, for example, the fear of missing out (Przybyski et al., 2013) and social media fatigue (Dhir et al., 2018, 2019), the academic comprehension of cyberstalking is comparatively at an early stage (Fissel, 2018). The measured growth of research on cyberstalking may be attributed, to a certain degree, to a lack of consensus for operationalized and conceptual recognition of cyberstalking as a distinct phenomenon (Dhillon and Smith, 2019; Fissel, 2018; Noble et al., 2014; Spitzberg, 2017). There seems to be an ongoing scholarly debate about potentially considering cyberstalking as a subset or perhaps extension of traditional stalking behavior due to comparable consequences (Worsley et al., 2017) and similar forms of potential interventions (Dreiling et al., 2014).

For example, cyberstalking is similar to traditional stalking in evocation of negative emotions (Worsley et al., 2017), trauma (Short et al., 2015), and fear of being victimized (Pereira and Matos, 2016) that results from intrusive communication patterns directed towards the victims (Chaulk and Jones, 2011; Short et al., 2014; Tokunaga and Aune, 2017). This debate is further compounded by a dearth of knowledge on the different forms in which cyberstalking can manifest. Only a limited number of studies have attempted to classify different forms of cyberstalking that an individual may perpetrate or experience (Begotti and Maran, 2019; Brown et al., 2017; Short et al., 2015; van Rensburg, 2017), such as intimate partner stalking (Marcum et al., 2018; Smoker and March 2017; Woodlock, 2017).

Scholarly uncertainty about the characterization and forms of cyberstalking has also resulted in a dearth of conclusive information on its prevalence in the general public (Pereira and Matos, 2016). While some studies have aimed to establish the prevalence of cyberstalking (Berry and Bainbridge, 2017; Dreiling et al., 2014; Fissel and Reyns, 2019; Gan, 2017; Maran and Begotti, 2019), findings have been divergent. For instance, Paullet et al. (2009) found 13% of respondents to be cyberstalking victims. Kraft and Wang (2010) found a prevalence rate of 9% among their respondents—but another study, conducted shortly thereafter, found a prevalence rate of almost 41% prevalence in the examined sample (Reyns et al., 2012). The dissimilarity of findings is too great to be dismissed. Some change in these studies’ prevalence rates could be attributed to the lapse of time, but these studies do not seem to reveal a coherent shift, especially as both studies were conducted in the context of the United States (USA). Similarly, Strawhun et al. (2013) reported that 20.5% of their respondents were victims of cyberstalking, whereas Dreiling et al. (2014) reported a prevalence of 6.5%. Berry and Bainbridge (2017) found 20–34% of respondents had experienced cyberstalking. More recently, Maran and Begotti (2019) found 46% of their respondents to have been cyberstalking victims. Further, DeKeseredy et al. (2019) reported 35% of respondents had been victims of technology-enabled stalking. In contrast, Fansher and Randa (2019) said only 10% of respondents had been stalked by a person they initially met through social media.

These studies suggest a clear lack of consensus on the prevalence of cyberstalking. This disparity may be attributed to various reasons, such as methodological differences (Reyns, 2019), lack of awareness about the attributes of cyberstalking (Smoker and March 2017), variations in reticence toward reporting such incidents (Cripps and Stermac, 2018), or even variation in demographic attributes of respondents such as gender (Maran and Begotti, 2019). The evident differences in findings of extant studies and the emergent nature of this research domain call for further research into investigating the multi-faceted and complex nature of cyberstalking (Fissel, 2018; Reyns, 2019).
3. Research method

In order to ensure the transparency and reproducibility of the present SLR (Tranfield et al., 2003), the study follows the review protocol suggested by Behera et al. (2019), as they developed highly comprehensive criteria for article assessment based on a robust review of previously published SLRs. The current SLR was conducted in two phases, (i) planning and execution of review; and (ii) development and reporting of the research profile as well as findings of the SLR (see figure 1). The first phase was focused on determining research objectives, identifying appropriate databases, and determining keywords and article selection (inclusion & exclusion) criteria for curating the study sample. To initiate the SLR, the following objectives were outlined to be met by the review:

RO1. To evaluate the research profile of the selected studies in term of publication trends, authors’ productivity, geographic scope, leading journals as well as publishers, prevalent research designs, targeted samples, and analytical techniques;
RO2. To identify the key research themes from prior studies on cyberstalking that have received scholarly attention;
RO3. To detect gaps and limitations of the selected studies and outline recommendations for future research;
RO4. To develop a comprehensive framework as a guideline for further study on cyberstalking based on identified gaps, limitations, and identified agendas for future research.

Two databases, Scopus and Web of Science (WoS), were chosen as appropriate databases based on their exhaustive coverage of peer-reviewed publications across multiple research domains and subjects (Minola et al., 2014). Appropriate keywords for this SLR were identified by executing a preliminary search on Google Scholar for the keyword “cyberstalking.” The first 50 search results, sorted based on relevance, were reviewed, and the variant terms “Internet stalking,” “online stalking,” “cyberstalking” and “cyber-stalking” were also found. Thus, Scopus and WoS databases were searched by combining these five keywords using the search syntax indicated in figure 1. To meet the objective of studying the evolution of cyberstalking in the past decade, only studies published from 2009 to 2019 were included. The search resulted in a total of 294 potentially relevant studies (139 from Scopus and 155 from WoS). Next, following recommendations of previous SLRs (e.g., Ain et al., 2019; Behera et al., 2019; Mehta and Pandit, 2018), specific article selection criteria were utilized to review the 294 studies. A study was included in the final sample for further analysis if it met the following inclusion criteria: (a) the term “cyberstalking” (or one of the equivalent terms mentioned above) was mentioned in abstract, keywords, or title, (b) cyberstalking was empirically investigated, (c) the study was published in a peer-reviewed journal, and (d) the full text of study was available in English. Concurrently, a study was excluded from further consideration if: (a) the focal area of study was related to legal, criminal, or judicial research domains, (b) the full text was unavailable in the database, (c) the study did not offer substantial insights into cyberstalking, (d) the study was published as a book, chapter in an edited book, conceptual review, thesis or conference paper, and (e) the study was a duplicate of an earlier search result.

Next, citation chaining (forward and backward) was performed to close the feedback loop and review any additional studies that could be considered for inclusion in the sample (Webster and Watson, 2002). Two authors conducted the review independently, and then discussed any conflicting results on article selection. The researchers reached a consensus on the final sample through mutual discussion and consent over every reviewed article’s appropriateness in meeting the selection criteria at all stages of the review. Fleiss’ Kappa value of 0.88 (Landis and Koch, 1977) was achieved, indicating strong inter-coder reliability. Ultimately, 49 studies were selected for inclusion. These, along with the reasons for their selection, were reviewed by a third author to ensure the robustness and unbiased nature of the sample (Behera et al., 2019; Kitchenham et al., 2009; Mehta and Pandit, 2018).

Next, two authors employed content analysis techniques to independently review the selected studies and explicate emergent research themes, gaps, and directions for future research. As with the article selection process, the two authors discussed their independent review results to reach a consensus on the research themes, gaps, and future agendas detailed in the following sections. In any case of conflict between the two authors, a third author reviewed the results to provide input needed to achieve a unanimous decision. The inter-coder reliability for the review process was satisfactory. Fleiss’ Kappa value of 0.84 (Landis and Koch, 1977) was achieved for inter-coder reliability.

Further, to derive the focal themes addressed by prior scholars, the authors utilized recommended processes for open, axial, and selective coding (Glaser and Strauss, 1967). In the open coding process, data derived from the reviewed studies were abstracted to formulate categories. Next, similarities and relationships among these categories were explicated to delineate more broad and major categories during the axial

Figure 1. SLR process & protocols. Note: The search syntax illustrated in the figure was for Scopus. The syntax was modified for WoS [TOPIC:(cyberstalking) OR TOPIC: (“internet stalking”) OR TOPIC: (“online stalking”) OR TOPIC: (“cyber stalking”) OR TOPIC: (“cyber-stalking”) but same limiting criteria were used.
coding process. Lastly, a selective coding process was undertaken to systematically identify the core categories of themes and develop the final themes discussed in section four (Zhang et al., 2020). Three authors independently completed the coding process, and the final themes reflected their unanimous categorization of the inappropriate themes. The inter-coder reliability for the coding process was deemed suitable (Kappa value of 0.88) (Landis and Koch, 1977).

3.1. Research profile

The selected studies were examined to determine the structure of extant research on cyberstalking. Results suggest that cyberstalking research is yet in its infancy as the number of empirical studies on this concept has grown significantly only in the past three years. Between 2009 and 2016, only a few studies seem to have focused on cyberstalking using an empirical construct ($n \leq 5$ per year). However, twice as many per year were conducted 2017–2019 ($n = 11$ in 2017 and 2018, $n = 9$ in 2019). This finding supports the contention of prior studies such as Smoker and March (2017) and Reyns et al. (2018), who indicate limited academic understanding and measurement scales for cyberstalking.

Investigation of the affiliations of first authors of reviewed studies and the geographic scope of research indicates that cyberstalking has been primarily investigated in developed countries such as the United

Figure 2. a. Keyword cloud (author indexed keywords). 2b. Keyword cloud (article titles)
States of America (USA) (n = 26), the United Kingdom (n = 6), Australia (n = 3), Canada (n = 3) and Malaysia (n = 3). There is a distinct lack of studies that examine cyberstalking in the context of developing countries such as India, the United Arab Emirates, and China, all of which have significant Internet/social media penetration (Statista, 2019). In terms of leading publications’ sources, the study sample suggests that the leading journal in terms of publication count is the Journal of Interpersonal Violence (n = 5). The majority of studies have been published by esteemed publishing houses such as Sage (n = 11), Springer (n = 7), and Taylor & Francis (n = 8). The leading authors in cyberstalking research, in terms of publication count, are Prof. B. W. Reynolds (Weber State University, USA) (n = 7), Prof. B.S. Fisher (University of Cincinnati, USA) and Dr. E. Short (University of Bedfordshire, United Kingdom). In terms of the prevalent research designs, the majority of studies seem to have focused on investigating cyberstalking in the context of students (n = 31) and used survey-based methodologies (n = 43). Also, prior studies present an equivalent adoption of analytical techniques that include univariate (n = 33) and multivariate (n = 23) analyses.

To gain further insights into the extant knowledge capital and intellectual structure of this research area, a word cloud was created for keywords (figure 2a) and titles of the selected articles (figure 2b). These suggest that the current research in this domain is focused around the popular keywords of “harassment,” “stalking,” “violence,” “victimization,” “students,” and “college.” These support the developed research profile in terms of sample focus and also coincide with the subsequently discussed research themes.

4. Results

The SLR employed content analysis techniques for reviewing the findings, results, and implications of the selected studies in order to identify four emergent research themes that have been the primary focuses of prior research.

4.1. Concept and form: comparison with traditional stalking

The search protocol and review suggest a significant variance in terms of existing definitions of cyberstalking in extant literature. Yet, for obtaining holistic comprehension of cyberstalking, it is important to understand its possible similarities and differences from traditional (i.e., offline) stalking. Thus, we have attempted to consolidate prior information in terms of conceptual differences and similarities of cyberstalking from traditional stalking, as discussed by prior scholars. Scholars argue that both forms of stalking are entwined in a complex way and may be mutually inclusive—for example, they may exhibit a direct association amongst themselves (Reyns and Fisher, 2018). However, it is also suggested that cyberstalking may be more prevalent (Reyns et al., 2012).

This review indicates inherent similarities between cyberstalking and offline stalking in terms of: (a) behaviors displayed by stalkers (Begotti and Maran, 2019; Short et al., 2014), albeit through different mediums (Begotti and Maran, 2019); (b) victims’ levels of social support and coping mechanisms (Begotti and Maran, 2019; Worsley et al., 2017); (c) self-protective behaviors (Nobles et al., 2014) and management tactics adopted to dissuade stalkers, such as responding in a verbally aggressive manner (Tokunaga and Aune, 2017); (d) psychological consequences experienced by victims (Worsley et al., 2017) such as psychological distress (Short et al., 2015); (e) stalkers’ profile e.g., employment and educational status (Cavezza and McEwan, 2014); (f) the influence of gender (Ahlgrim and Terrance, 2018; Reynolds, 2019; Reynolds and Fisher, 2018; White and Carmody, 2018); and (g) targeting of multiple victims (Cavezza and McEwan, 2014).

Contrarily, the following differences have been observed between cyberstalking and offline stalking: (a) the form and channel of stalking (Cavezza and McEwan, 2014), such as technical privacy invasion in cyberstalking vis-à-vis physical invasion/violence in offline stalking (Short et al., 2014); (b) differential motives, tactics and methods for perpetration (Reyns, 2019; Reynolds et al., 2018). For example, lack of self-control instigates cyberstalking more than offline stalking (Reyns et al., 2018); (c) victim-offender relationship (Short et al., 2014). For example, victims may be aware of the identity of an offline stalker, but not a cyberstalker who can use technology to obfuscate their identity (Short et al., 2014); (d) comparatively more intimidating influences for cyberstalking victims (Brown et al., 2017). This last difference may be attributed to the fact that cyberstalking victims gradually experience fear and perceive a lack of immediate threat. In contrast, offline stalking victims may immediately feel threatened or fearful (Nobles et al., 2014). This also influences victims’ time taken to initiate self-protective actions (Nobles et al., 2014).

4.2. Antecedents

Scholars have investigated cyberstalking incidences from multiple perspectives, including victims’, cyberstalkers’ (also referred to as perpetrators), and the points-of-view of societal members such as peers, online service providers, parents, etc. We posit that these individuals encompass different stakeholders affected by cyberstalking incidences. The previous literature has examined multiple factors associated with these stakeholders that can directly or indirectly influence cyberstalking. For example, prior studies have examined whether the experience of relational difficulties such as deviant peer associations (DeKeseredy et al., 2019; Marcum et al., 2014, 2017; Navarro et al., 2016) and interpersonal jealousy (Strawhun et al., 2013) may influence the degree and duration of cyberstalking. Further, previous studies have implied that both victims and perpetrators may be influenced by factors associated with using of internet/social media and socio-demographics. We discuss these factors in terms of the perpetrator, victim, and the roles of online social media service providers, and parents.

4.2.1. Profile

Based on our review, we identify different aspects of individual cyberstalkers (i.e., offenders or perpetrators) and victims that have received scholarly attention. We posit that these aspects may be understood as elements of a general profile for stalkers and victims.

4.2.1.1. Perpetrator. Extant literature has primarily focused on identifying cyberstalkers’ traits through a study of their personality traits, personal attributes, and internet/social media usage tendencies.

(i) Personality and motivation

Few studies have examined the personality traits of a perpetrator, for example: machiavellianism (Smoker and March 2017), sadism (Kiracaburun et al., 2018; Smoker and March 2017), narcissism (Kiracaburun et al., 2018; Menard and Pincus, 2012; Smoker and March 2017), degrees of lack of self-control (Marcum et al., 2014, 2017; Reyns, 2019; Reynolds et al., 2018), general psychopathy (Smoker and March 2017), fearful attachment style (Strawhun et al., 2013) as well as physical and sexual aggression (Strawhun et al., 2013).

Further, previous studies have suggested that personality traits and personal factors can also act as motivators for perpetration of cyber-stalking. For example, anger (Strawhun et al., 2013), discomfort with
intimacy (Ménard and Pincus, 2012), desire for immediate gratification (Fansher and Randa, 2019), and fulfilling the need for social risk-taking (Welsh and Lavoie, 2012) have been found to motivate cyberstalkers. Additionally, Ménard and Pincus (2012) suggest that perpetrators may also be driven by experiences of traumatic or sexual abuse, and may be associated with alcohol expectancies.

(ii) Socio-demographic factors

Prior investigations into cyberstalking indicate that cyberstalkers tend to be younger (Reyns et al., 2012), educated, well-performing, and more technologically sophisticated than other types of stalking offenders (Navarro et al., 2016).

Previous research has presented evidence of significant gender differences in cyberstalking perpetration. For example, males have been more commonly identified as perpetrators (Ahlgrim and Terrance, 2018; Fansher and Randa, 2019; Pereira and Matos, 2016) vis-à-vis females (Strawhun et al., 2013) and are also reported to be comparatively more dangerous (Ahlgrim and Terrance, 2018). In the context of intimate partner stalking, Smoker and March (2017) suggest a higher likelihood of perpetration by females, whereas Marcum et al. (2017) report that men are more prone to engage in repeated attempts to login into partners’ accounts. Gender differences have also been noted for personal and personality-related factors that can prompt cyberstalking. Previous research has determined that for males, cyberstalking tendencies may be predicted by machiavellianism (Kircaburun et al., 2018), narcissism (Ménard and Pincus, 2012), problematic attachment style (Ménard and Pincus, 2012; Strawhun et al., 2013), anger (Ménard and Pincus, 2012), and physical aggression (Strawhun et al., 2013), whereas for females, cyberstalking may be predicted by narcissism (Kircaburun et al., 2018), interpersonal jealousy (Strawhun et al., 2013), sexual abuse (Ménard and Pincus, 2012), anger (Strawhun et al., 2013), and intimacy discomfort (Ménard and Pincus, 2012).

(iii) Internet/social media usage characteristics

Strawhun et al. (2013) suggest that an increase in the amount of time spent online can enhance an individual’s chances of engaging in cyberstalking. Further, studies also indicate that cyberstalkers may exhibit deviant behaviors related to problematic use of internet/social media such as sexting (Reyns, 2019) and cyber-harassment (Al-Rahmi et al., 2019). And yet, only limited attention has been given to examining perpetrators’ problematic and excessive engagement with the internet or social media (Al-Rahmi et al., 2019; Navarro et al., 2016). Based on the review, we argue for this to be a gap that critically needs greater attention.

4.2.1.2. Victim

Previous studies have focused significant attention on explicating socio-demographic and social media/internet usage characteristics of victims.

(i) Socio-demographic factors

Socio-demographics factors, e.g. locational proximity to the perpetrator (Reyns et al., 2011); have been suggested to significantly influence an individual’s likelihood of experiencing cyberstalking, but the findings present some inconsistencies. In terms of age, Short et al. (2015) and Lohbeck and Petermann (2018) suggest higher odds for the stalking of older individuals. Further, age can cause individuals to perceive cyberstalking differently (Reyns, 2019) and has also been posited to neutralize gender differences in both cyberstalking victimization and perpetration (Strawhun et al., 2013). Probability of victimization has been further suggested to be influenced by education level, income (Nobles et al., 2014) and educational status (Nobles et al., 2014). Further, Reyns et al. (2012) suggest that non-Caucasians, non-heterosexuals, and individuals in a relationship are more likely to experience cyberstalking.

Significant gender differences have also been identified in victims’ experience and reporting of cyberstalking. Males may show a higher propensity to engage in risky behaviors that can promulgate cyberstalking, but they experience less victimization (Fansher and Randa, 2019; Gan, 2017; White and Carmody, 2018). Male victims may be less likely to report their victimization (Berry and Bainbridge, 2017) and experience more school-related consequences (Fissel and Reynolds, 2019). Males have also been found to suffer more adverse consequences due to stalking perpetrated by female ex-intimate partners (Fissel and Reynolds, 2019), as such females may be more mentally unstable than a stranger (Ahlgrim and Terrance, 2018). Further, a few studies suggest that men (Spitzberg, 2017) and individuals outside the traditional gender classification (Fissel, 2018), e.g., transgendered individuals, were more likely to acknowledge and report cyberstalking incidences. Females have been found to have a much higher probability of victimization (Paullet et al., 2009) and suffer more consistently from cyberstalking (Dreiling et al., 2014; Pereira and Matos, 2016; Reyns et al., 2012). Female victims also generally perceive cyberstalking as more harmful (Gan, 2017). They are likely to experience work-related as well as social consequences (Fissel and Reynolds, 2019), but their reporting of cyberstalking incidences may be taken less seriously than instances reported by male victims (Gan, 2017). Contrarily, Dreiling et al. (2014) posit gender differences do not affect victims’ experienced consequences, and Berry and Bainbridge (2017) report an equal likelihood of both genders to be victimized.

(ii) Internet/social media usage characteristics

Studies indicate that victims’ usage patterns and their levels of engagement with the internet or social media (Paullet et al., 2009), e.g., the degree of disclosure of information on online platforms (Fansher and Randa, 2019; Welsh and Lavoie, 2012), can influence their cyberstalking experience. Frequent or prolonged use of the internet has been posited to increase the likelihood of being cyberstalked by strangers (Berry and Bainbridge, 2017; Gan, 2017). Berry and Bainbridge (2017) also suggest that experienced internet users may have a higher tendency to be cyberstalked as compared to inexperienced users.

4.2.2. Social media and technological platforms

Technology-enabled communication platforms, such as social media, and smart devices such as smartphones, have been acknowledged as a cause for rising cyberstalking incidences (Chaulk and Jones, 2011; Fansher and Randa, 2019; Welsh and Lavoie, 2012), can influence their cyberstalking experience. Frequent or prolonged use of the internet has been posited to increase the likelihood of being cyberstalked by strangers (Berry and Bainbridge, 2017). This may be attributed to two reasons. First, they enable stalkers to establish a pervasive presence around potential and actual victims (Woodlock, 2017). Second, the type of activities an individual may engage in on the internet or social media platform such as Facebook (Chaulk and Jones, 2011), and the length of such engagement may also increase victims’ proclivity to experience cyberstalking (Berry and Bainbridge, 2017), for example, by facilitating social media contact with a stalker (Fansher and Randa, 2019). Thus, it may be said that individuals’ usage patterns, and frequencies of technology-enabled platforms, such as social media, may be making individuals more vulnerable to cyberstalking.

Social media platforms are being especially recognized for facilitating cyberstalking in relative anonymity, even without victims’ knowledge. For instance, Facebook users have no way to know who visits their profile or the frequency of such visits, allowing stalkers to access such information and gain knowledge. For instance, Facebook users have no way to know who visits their profile or the frequency of such visits, allowing stalkers to access such information and gain knowledge. Social media platforms are being especially recognized for facilitating cyberstalking in relative anonymity, even without victims’ knowledge. For instance, Facebook users have no way to know who visits their profile or the frequency of such visits, allowing stalkers to access such information and gain knowledge.
inappropriate content posted by a stalker on a victim’s profile could be easily visible to their friends, families, and social connections (Nobles et al., 2014). This can have dual connotations for victims. On the negative side, it can create an indelible impact on their reputation and psychological well-being; whereas, on the positive side, victims can quickly initiate self-protective actions, vis-à-vis traditional stalking situations (Nobles et al., 2014).

4.2.3. Role of stakeholders

(i) Parents

Extant research suggests that parents can play a significant role in helping adolescents and young adult victims to cope with cyberstalking. For instance, Wright (2018) determined that parental support negatively correlates with cyberstalking and influences victims’ experienced consequences, such as depression and academic performance. Thus, parental involvement can increase the probability of an adolescent victim’s reporting of incidents and expression of fears associated with cyberstalking (Pereira and Matos, 2016).

(ii) Online service providers

Prior cyberstalking literature has discussed potential ethical responsibilities of online third-party platforms where cyberstalking incidents towards victims are perpetrated (Al-Khateeb et al., 2017; Dhillon and Smith, 2019). Dhillon and Smith (2019) report that individual users of such platforms feel that service providers have an ethical responsibility to compel all users to comply with appropriate societal and digital communication norms. Further, these online service providers have access to critical information about cyberstalking incidents, which could be used to apprehend offenders and assist victims in mitigating current, or avoiding future occurrences (Al-Khateeb et al., 2017). This information could be used to develop countermeasures and policies against cyberstalking, such as refusal of service to reported cyberstalking offenders (Dhillon and Smith, 2019). It would be relatively easier for service providers to develop and enforce anti-cyberstalking policies compared to formal legal and judicial systems. Such actions could also help service providers improve customer satisfaction and gain a potential market advantage (Al-Khateeb et al., 2017), by publicly fulfilling ethical and moral obligations towards society.

4.3. Consequences and outcomes

The literature has extensively examined the consequences or outcomes of cyberstalking, especially from victims’ perspectives, and has been found to affect their personal as well as professional lives (Fissel and Reynolds, 2019; Short et al., 2015; Worsley et al., 2017). Based on our review, we propose three characterizations of functional, physiological, and psychological consequences.

(i) Functional.

Cyberstalking victims can experience adverse functional consequences, e.g., lowered academic performance (Wright, 2018) that significantly disrupt their daily lives (Perreira and Matos, 2016; van Rensburg, 2017). Victims’ may also be aggrieved by increased financial costs. At the same time, they cope with cyberstalking due to multiple reasons such as geographical relocation, attorney fees, damage to property, child-care costs, switching telecom operators, etc. (Nobles et al., 2014; Short et al., 2015; Woodlock, 2017).

(ii) Physiological.

Only a limited number of studies have focused on investigating physiological consequences that may be experienced by victims. Yet these studies posit that cyberstalking can induce significant changes in victims’ daily activities such as eating and sleeping (Short et al., 2015) and cause issues such as fatigue (Begotti and Maran, 2019) and severe sleep disturbances (van Rensburg, 2017).

(iii) Psychological.

The majority of reviewed studies have determined that cyberstalking can cause significant detriment to victims’ psychological well-being (Dreiling et al., 2014), by inducing mental (Short et al., 2015; Worsley et al., 2017) and emotional distress (Brown et al., 2017; Cripps and Stermac, 2018). Cyberstalking has been found to be associated with victims’ experience of negative emotions such as prolonged worry (van Rensburg, 2017), chronic low mood (Worsley et al., 2017), fear (Brown et al., 2017; Morris et al., 2019), irritability (Short et al., 2015), helplessness (Worsley et al., 2017), depression (Begotti and Maran, 2019; Cripps and Stermac, 2018; Maran and Begotti, 2019; Wright, 2018), and anxiety (Brown et al., 2017; Cripps and Stermac, 2018; Worsley et al., 2017). Further, victims may consequently exhibit poor concentration on work, academic or social activities (van Rensburg, 2017), and develop a skeptical or suspicious nature (Brown et al., 2017). Researchers have also posited that some victims may also develop post-traumatic stress disorder (Cripps and Stermac, 2018; Morris et al., 2019; Short et al., 2015; Wright, 2018). Such consequences can induce victims to withdraw (Brown et al., 2017) and isolate themselves (Short et al., 2015) from social groups, e.g., by closing social media accounts (Woodlock, 2017).

Additionally, a few scholars have focused on studying how stalkers are affected by their own cyberstalking. These scholars posit that cyberstalkers may exhibit other deviant behaviors associated with maladaptive and problematic social media usage (Kircaburun et al., 2018), such as cyberbullying (Al-Rahmi et al., 2019) and sexting (Woodlock, 2017).

4.4. Strategies for reporting, coping, and prevention

4.4.1. Reporting

Prior research has extensively examined victims’ formal and informal reporting as well as help-seeking behaviors, and found that many man many victims choose not to report cyberstalking incidents (Berry and Bainbridge, 2017; Gan, 2017). This may be attributed to multiple reasons. For example, victims may be unable to formally recognize a cyberstalking incident, and consider it to be harmless (Gan, 2017) or unworthy of being reported (Berry and Bainbridge, 2017; Gan, 2017). Fissel (2018) suggests that victims usually report incidences and seek help if the stalking has occurred over a longer duration, or if they share a close relationship with the stalker.

Further, the consequences (e.g., on work, school, or health) experienced by a victim are contingent on the types of assistance sought by them (i.e., professional or informal help-seeking strategies) (Fissel, 2018). Victims may be more inclined to adopt informal strategies (Fissel, 2018); and the review suggests that victims’ personal and socio-demographic characteristics may influence this choice. For example, students may refrain from reporting and seeking help from police (White and Carmody, 2018) due to their conception that this would result in more negative consequences for themselves (Worsley et al., 2017). Further, Al-Khateeb et al. (2017) suggest that victims may show a willingness to seek private resolution with third-parties, e.g., from the service providers of platforms where cyberstalking occurred. The authors attribute this willingness to reasons such as the desire to avoid legal actions against offenders, self-blame, stalkers’ lack of intent to cause harm, and inadequate legal support due to perpetrators’ anonymity and lack of evidence. In some cases, stalkers’ characteristics may also influence the resolution of an incident; e.g., cyberstalking perpetrated by females was perceived to be easily resolvable (Strawhun et al., 2013).
To cope with cyberstalking, victims can utilize different strategies and self-protective actions (Nobles et al., 2014). Based on our review, we identified three distinct forms of coping strategies.

(i) Avoidance or ignorance strategy.

In some cases, victims may avoid the use of a technology (i.e., internet or social media) to increase the amount of effort that stalkers would have to make to further pursue such behaviors, thus potentially dissuade stalkers from continuing the stalking. This may include limiting or blocking stalkers’ access to information (Begotti and Maran, 2019; Tokunaga and Aune, 2017).

(ii) Confrontation strategy.

Vicims may exhibit a defiant reaction toward their stalkers to end the stalking (Begotti and Maran, 2019). According to Tokunaga and Aune (2017), victims can display varying confrontational hostility levels that may range from derogatory verbal aggression to pleading. But the effectiveness of such coping strategies still needs to be determined (Begotti and Maran, 2019). For instance, Tokunaga and Aune (2017) report that confronting stalkers directly through verbal aggression is least effective and could result in dire consequences for victims.

(iii) Support seeking strategy.

Kraft and Wang (2010) suggest that victims often cope with stalking by seeking support from their social circle (family, friends, partners, or spouses) and clinical practitioners (clinicians, psychologists, or therapists). Victims who adopt this strategy may also find it helpful to report the incident to a central system (e.g., email to service provider) for possible resolution (Kraft and Wang, 2010). Additionally, victims can seek assistance and protection from legal authorities, such as police (Begotti and Maran, 2019; Iqbal and Jami, 2019; Maran and Begotti, 2019; Worsley et al., 2017). However, this is dependent on multiple factors, including the form and severity of cyberstalking (Tokunaga and Aune, 2017), resilience and vulnerabilities of the victim (Worsley et al., 2017), and ease of reporting (Begotti and Maran, 2019; Maran and Begotti, 2019), to name a few.

4.4.3. Prevention

Scholars have shown a limited focus on discussions of effective strategies for the prevention of cyberstalking. Paulelt et al. (2009) suggested several ways that could potentially prevent cyberstalking, such as (i) avoiding the use of real names, nicknames, or suggestive names in online platforms, (ii) practicing caution prior to information disclosure on online platforms, and considering its ramifications in real-life scenarios, (iii) considering the potential for perpetual preservation and quick dissemination of information disclosed on online platforms, (iv) an immediate cessation of communication upon inappropriate contact, (v) record-keeping of all communication with a stalker, and (vi) reporting the incidence to internet service provider, law enforcement agency, school administration, etc. Further, Dhillon and Smith (2019) argue that the scope of such prevention strategies evolves in concurrence with changes in technological platforms and digital space. The authors defined specific objectives for preventing cyberstalking efficiently and effectively, such as preventing inappropriate online interactions, enhancing security procedures, and ensuring technical security.

5. Research gaps and future research directions

Limitations acknowledged by prior studies were assimilated; and similar to other fields in social sciences, the review indicates a substantial acknowledgment of methodological limitations in cyberstalking research. Further, we also identify four gaps in current literature regarding conceptualization, profiles as well as behaviors of victims and stalkers, roles of the digital environment, and of online service providers. These gaps and limitations have been used to delineate potential areas for future research that are also detailed in the following subsections.

5.1. Methodology and measurement

Issues related to the choice of research methodology have been acknowledged as a significant limitation by prior studies (Al-Rahmi et al., 2019; DeKeseredy et al., 2019; Morris et al., 2019; Reins et al., 2012; Tokunaga and Aune, 2017; van Rensburg, 2017; Wright, 2018), and have been posited to affect the generalizability of results (Al-Khateeb et al., 2017; Fissel and Reins, 2019; Navarro et al., 2016; Reins and Fisher, 2018; Spitzberg, 2017). The first of these reported issues relates to the use of cross-sectional surveys (Fansher and Randa, 2019; Reins, 2019), which extrapolate respondents’ behavior based on data collected at a single point of time. Such extrapolation causes problems in establishing causal and temporal associations between investigated variables (Fansher and Randa, 2019; Reins, 2019). Second, a few researchers have debated the use of qualitative research methods, which can offer rich insights regarding cyberstalking (Al-Rahmi et al., 2019) although such methods may present a risk of subjective bias (Dhillon and Smith, 2019).

Third, the techniques adopted for data collection could also influence findings of a study (Woodlock, 2017), e.g., reliance on self-reported data (Al-Khateeb et al., 2017; Smoker and March 2017; Worsley et al., 2017; Wright, 2018). Self-reported data has been implicated in reflecting social desirability biases, which can affect the scientific credibility of results (Spitzberg, 2017). Additionally, Reins (2019) acknowledged the limitations of using old data (e.g., collected more than ten years ago) to explicate cyberstalking behaviors, in that they may fail to capture the latest trends in technology. However, the authors argue that their findings are compatible with more recent studies.

Fourth, our SLR also indicates challenges pertaining to small sample sizes (Strawhun et al., 2013; van Rensburg, 2017; White and Carmody, 2018), and unbalanced samples in terms of age (Fissel, 2018) and gender (Kircaburun et al., 2018; Reins et al., 2012). Such issues are significant limitations, as social media users from different cultural and socio-demographic backgrounds might have unique cultural practices, including different communication norms, social standards, and perceptions of the criminal justice system (Fissel, 2018).

Fifth, very few studies have acknowledged limitations related to framework modeling, such as the small effect size of investigated associations (Marcum et al., 2018) and failure to produce standardized estimates (Reins et al., 2018). Our review indicates that construct measurement as well as the scope of investigated constructs are also important limitations acknowledged by prior scholars. For instance, Fissel and Reins (2019) state that failure to consider overlap or relationships between offline and cyberstalking victimizations is a significant limitation that subdues researchers’ ability to explain an empirical distinction between the two concepts. Furthermore, a respondent’s failure to acknowledge victimization can affect the measurement of cyberstalking (Fissel, 2018). Researchers have also noted measurement issues related to reliance on a single measure and/or limiting examination to a specific behavior (Navarro et al., 2016), or the utilization of a new and unvalidated scale (Smoker and March, 2017). Further, Reins and Fisher (2018) acknowledge limitations in examining a broader range of variables associated with cyberstalking that could add to current knowledge on this phenomenon. Such variables may include both predictors, such as sexual orientation (Maran and Begotti, 2019), impulsivity and risk-taking (Ménard and Pincus, 2012), as well as consequences, such as coping strategies (Maran and Begotti, 2019), financial loss, varied impacts on victims’ health (mental and physical), (Fissel and Reins, 2019) and so on.
5.1. Directions for future research

Future scholars may address these methodological limitations in four main ways. They should first validate extant findings through more cross-national and cross-cultural studies with representative samples that include respondents from different age groups, nationalities, cultural backgrounds, etc. (Al-Rahmi et al., 2019; Fissel, 2018). Scholars may also consider utilizing clinical samples with pre-identified cyberstalkers and victims to generate a more nuanced understanding of cyberstalking and its effects on both offenders as well as victims. Second, we posit the need to validate scales that have already been developed to measure cyberstalking. For example, Smoker and March (2018) developed a new scale for measuring cyberstalking, which resulted in good fit indices for the sample investigated in their research, and was carefully designed to avoid social desirability bias through use of careful wording. Future studies may focus on cross-cultural and cross-demographic intensive validation of such proposed scales.

Third, scholars need to adopt a narrow focus to explicate the dissimilarities between cyberstalking and offline stalking (e.g., factors that may drive behaviors) (Reyns, 2019). Thus, future researchers should consider using more rigorous research methodologies (e.g., longitudinal or mixed-method research) to better understand cyberstalking (Kircaburun et al., 2018). Further, scholars may also benefit from considering a time-based or temporal approach to the design of research methodologies. This would be beneficial, as a victim’s perception of a cyberstalking incidence may change over time, partially in conjunction with dynamic changes in the technological environment of social media platforms. That is, researchers may attempt to gather information from victims over a longer time (e.g., over five years) (Begotti and Maran, 2019). By collecting data at multiple points in time, they may also avoid loss of information due to memory lapses.

Fourth, researchers could study the degree to which stalkers and victims are influenced by demographic variables apart from age and gender, especially but not limited to occupation and education. We argue that such an examination would lead to development of more nuanced Stalker and victim profiles. Additionally, very few studies have examined the mediating and moderating influences of socio-demographic variables such as age, gender, and education level (Al-Rahmi et al., 2019; DeKeseredy et al., 2019; Reynolds, 2019). We argue for further research on explicating the mediating or moderating influence of socio-demographic variables on cyberstalking, its antecedents, and consequences.

5.2. Theoretical foundations and grounding

Our review indicates a lack of a unified conception of cyberstalking (e.g., Maran and Begotti, 2019). Due to conflicting information about the behaviors that constitute cyberstalking (Ahlgrim and Terrance, 2018), researchers have called for the development of a clear and universal definition of cyberstalking (Spitzberg, 2017). Through this review, we delineate that cyberstalking incorporates the use of technology-enabled devices (computers, smartphones, etc.) and platforms (e.g., email, messaging, social media) to continually gather information on the targeted individual. Such stalking behavior may be both passive (e.g., information gathering) as well as active (e.g., violence or harassment), and may induce emotions of fear or anger in the stalked individual (i.e., the victim). Furthermore, we argue that a gap exists in considering reports from civic stakeholders affiliated with victims (e.g., parents and peers) who are consequentially, even if indirectly, affected by cyberstalking. Another limitation in the context of cyberstalking research pertains to the influence of socio-cultural aspects. In seminal literature on offline stalking, scholars have indicated that variables such as social anxiety and relational instability can be conduces to the emergence of stalking behaviors (Mullen et al., 2001). However, a more recent study indicated that national attitudes specific to gender could better predict traditional stalking (Sheridan et al., 2019). Due to the current inconsistency in the examination of socio-cultural factors specific to cyberstalking, we borrow from the literature on traditional stalking to argue for a gap in examining the influence of national and regional attitudes as well as cultural and sub-cultural norms on cyberstalking perpetuation and prevalence.

Additionally, Dhillon and Smith (2019) indicate the need to gather systematic and theoretically-driven information on cyberstalking as a relatively new phenomenon. Reynolds et al. (2018) also suggest that the extant literature provides little information about theoretically-driven cyberstalking predictors. The current review supports this contention, as few reviewed studies have utilized existing theories in developing frameworks (e.g., Dhillon and Smith, 2019; Fissel, 2018; Kircaburun et al., 2018). This indicates a gap in the theoretical grounding of the concepts of cyberstalking research.

5.2.1. Directions for future research

We propose a three-fold approach for scholars to address these gaps.

(i) Improving theoretical foundations and conceptualization of cyberstalking.

Qualitative and comparative studies across different user cohorts demarcated by demographic indicators (e.g., education, occupation, age, and gender) (Maran and Begotti, 2019), should be conducted to develop a more nuanced understanding about differences in individual perceptions and/or assessments of cyberstalking. We also posit the need to investigate the influence of socio-cultural factors on cyberstalking, such as family structure, ethnic values and beliefs. Based on our SLR findings, we propose that socio-cultural factors (e.g., national/ regional attitudes, cultural norms etc.), and demographic indicators (e.g., occupation, income, etc.) would influence victims’ response as well as coping mechanisms. For example, studies may be oriented to understand the degree to which female victims in patriarchal cultures hesitate in reporting cyberstalking due to fear of negative backlash or fear of damaging their social reputations. Such understanding could also lend further insights into cyberstalking’s nature and its difference from offline stalking (Begotti and Maran, 2019). Further, researchers may examine the association of cyberstalking with other phenomenon associated with the dark side of social media, such as social media fatigue (Dhir et al., 2018, 2019) and social media-induced jealousy (Rus and Tiemensma, 2017). This would allow scholars to holistically understand the interactivity of associations among various online deviant behaviors categorized as the dark side of social media.

(ii) Espousing robust theoretical grounding.

Future scholars would benefit from utilizing pre-existing, seminal theoretical models from the psychology, management, and consumer behavior literatures, such as the stressor-strain-outcome model (SSO, Koeske and Koeske, 1993), theory of compensatory internet use (TCIU, Kardes-Winter, 2014), theory of planned behavior (TPB, Ajzen, 1991), and theory of reasoned action (TRA, Fishbein and Ajzen, 1975), all of which have been previously used in social media research (Elhai et al., 2020; Lin, 2015; Salo et al., 2019). The further utilization of such theories would enable scholars to develop frameworks that could generate more standardized and holistic explanations for victims’ intentions in response to cyberstalking. Further, theories such as behavioral reasoning theory (BRT, Claudy et al., 2015) and self-determination theory (SDT, Deci and Ryan, 1985) may be adapted to better understand better perpetrators as well as victims, e.g., (a) victims’ intention to respond to cyberstalking and reasons thereof, (b) stalkers’ reasons for perpetrating cyberstalking and their intentions to use social media platforms for the same.

(iii) Adopt a multi-stakeholder perspective.

Based on the findings, we posit that the theoretical foundations of
cyberstalking would be strengthened by considering inputs from multiple stakeholders that include stalkers, victims, and social/peer and/or familial groups. It is our contention that the theories like SSO, BRT, TCMI and TRA may also be used to understand intention—behavior gaps in responding to cyberstalking from a multi-stakeholder perspective. The adoption of a multi-stakeholder perspective, as well as a multi-disciplinary outlook along with the use of theoretically grounded frameworks, will enable future scholars to explain the apparent inconsistencies between victims’ responses, contingent to stalkers’ attitudes, intentions, and behaviors.

5.3. Victims: Profile and behavioral responses

We delineate some aspects of victims’ psychological and socio-demographic profiles that would benefit from scholars’ closer attention (Ahlgrim and Terrance, 2018; Fissel, 2018). For example, only limited attention has been given to understanding cyberstalking among sexual-orientation minorities. Also in terms of socio-demographics, few scholars have considered examining the effects on behavior of financial costs experienced by cyberstalking victims (Paullet et al., 2009), associated with changing service providers, geographical relocation, and so on. We argue this is an important gap in the literature, as there is a possibility that such financial costs can influence victims and exacerbate other psychological consequences of cyberstalking.

Although prior literature has given sufficient attention to understanding victims’ responses to cyberstalking, the findings of our SLR indicate some distinct knowledge gaps. For instance, there is a limited understanding of victims’ behavioral responses regarding third-party support-seeking and self-protection. The literature also seems unable to provide clear knowledge of how victim-offender relationships (Begotti and Maran, 2019; Reys, 2019) affect cyberstalking vis-à-vis offline stalking incidences (Tokunaga and Aune, 2017). Further, there is little information on the differential degree of intensity of victims’ emotions, contingent to methods, channels, and tactics utilized by cyberstalking perpetrators. These limitations signify substantial gaps in our understanding of how victims respond to a stalker and a cyberstalking incident.

Additionally, DeKeseredy et al. (2019) discussed the need for new prevention and intervention strategies to assist victims in coping with cyberstalking victimization. We concur and argue for the need to explore individual behaviors that victims may adopt for self-protection and their interactions with victims’ response or coping strategies. These findings also further delineate the gap in understanding how socio-demographic differences (e.g., culture, age, gender, and education) affect victims’ individual behavior.

5.3.1. Directions for future research

Future researchers must derive more nuanced insights about how victims react to and cope with cyberstalking victimization especially in terms of their behavioral as well as emotional responses (Fissel, 2018). This knowledge may help scholars in devising protective strategies that can help victims to counteract cyberstalking, e.g., by obtaining information from victims on their response to specific practices adopted by cyberstalkers (Reys and Fisher, 2018).

Further, among the socio-demographic variables that are under-investigated, in terms of cyberstalking, is age. Comparative studies could also be conducted to understand how age differs in their perception and/or assessment of cyberstalking with regards to potentially confounding variables in educational (e.g., college vs. non-college) and occupational status (employed vs. non-employed).

Scholars should especially investigate the element of fear regarding cyberstalking victimization and the degree to which its influence differs for cyberstalking vis-à-vis offline stalking victims (Reys et al., 2018). This is in concurrence with the proposition of Pereira and Matos (2016), who suggests that future research should focus on providing effective and meaningful paradigms to assist victims in coping with cyberstalking irrespective of their level of experienced fear. Next, future researchers may consider investigating the impacts of legal, economic, and socio-cultural contexts on victims’ adopted self-protective as well as incidence reporting responses. This could enable researchers to determine whether victims consider reporting to be a protective barrier that would deter a cyberstalker. These studies could also determine the degree of systemic trust placed by victims in legal or social systems, which could help us understand how to encourage reporting of cyberstalking incidences.

5.4. Stalkers’ behavior

Extant research has paid comparatively lesser attention to cyberstalkers, and there are considerable limitations in current knowledge on cyberstalkers’ emotional, affective and behavioral profiles. For instance, studies have indicated low self-control to be a significant predictor for perpetrators’ engagement in cyberstalking (Reyns, 2019; Reyns et al., 2018). But our review indicates a gap in understanding how self-control is perceived by stalkers themselves and the degree of its influence on cyberstalking.

Another issue that has seen limited investigation pertains to third-party stalking, that is, cyberstalkers’ ability to motivate others to stalk the same victim. This is a reportedly common behavior among cyberstalkers (Ahlgrim and Terrance, 2018), which can prove to be dangerous, even fatal, considering that it can compound the degree and impact of adverse consequences for victims and needs to be explored further (Ahlgrim and Terrance, 2018).

5.4.1. Directions for future research

We implore scholars to consider seminal studies on traditional stalking (Mullen et al., 1999; Sheridan et al., 2003) while developing a profile of cyberstalkers, especially in terms of their affective, personality, and emotional traits. Scholars might also conduct cross-cultural and comparative studies to develop universal profiles of cyberstalkers. Such profiles can be publically disseminated to assist individuals in identifying potential stalkers, especially in regions that, as mentioned above, have not been the direct focus of research. Further, scholars may focus on understanding the prevalence of third-party stalking; as well as the behavioral traits of a cyberstalker that enable them to induce third-party stalking. This knowledge can assist researchers in developing deeper insights about stalkers’ ability to develop novel ways to perpetuate cyberstalking.

5.5. Digital environment: social media and online service providers

Navarro et al. (2016) have determined an empirical association between internet addiction and cyberstalking. Following this, we posit a gap in explicating the link between cyberstalking and other deviant online behaviors, such as social media fatigue (Dhir et al., 2018), jealousy (Frampton and Fox, 2018), relational intrusion through online platforms (Chaulk and Jones, 2011), etc. We argue that this gap is critical due to the continual evolution of the technological environment that can broadly affect cyberstalkers’ and victim’s experiences. Further, previous studies report that victims may desire to seek third party resolution, e.g., from service providers of the online platforms where cyberstalking occurred. However, there is limited information on the perspective of such service providers on cyberstalking and their stances towards promulgating its discontinuance. This is another significant gap in the literature, since such service providers may possess important information on individual cyberstalking incidents which could assist victims in pursuing formal or legal recourse as a response strategy, either individually or through victim protection groups.

5.5.1. Directions for future research

Future scholars may focus on understanding how cyberstalking is associated with other online deviant behaviors classified as the dark side...
of social media, for example, through the application of the honeycomb framework (Baccarella et al., 2018; Talwar et al., 2020), to enhance their understanding of this phenomenon. It would also assist in developing a more comprehensive understanding of the dark side of social media (Mantymaki and Islam, 2016; Talwar et al., 2019), and generating insights about the interactive effect of a specific online deviant behavior (e.g., cyberstalking) in inducing perpetration of other negative behaviors (e.g., online harassment, relational intrusion). Further, future research should also focus on new victimization risks created due to the prolific use of social media and/or technology, as well as influences on victims’ coping mechanisms and response strategies (Maran and Begotti, 2019; Fansher and Randa, 2019). Such research efforts would yield information that could be used to develop awareness and educational programs to aid victims and potential victims about the safe use of online platforms and deterrence of cyberstalkers. Lastly, future research should intensively explore the role of the responsibility of online service providers with respect to cyberstalking, as their involvement in adherence with data protection laws may offer support to the development of effective legal resources and intervention strategies that protect victims’ privacy (Al-Khateeb et al., 2017). Such studies should also focus attention on the existing barriers that may prevent online service providers in providing assistance and/or information for inhibiting cyberstalking.

5.6.Synthesized research framework

To assist scholars and contribute to expanding intellectual boundaries of cyberstalking research, we propose a framework that synthesizes the key avenues, associations, and constructs identified above as emergent avenues for future research (see Figure 3). Based on the gaps described above, the following avenues are suggested as guidance for systematic studies of cyberstalking in form of a potential framework. First, as described above, we argue for the need for methodological advancement and more theoretical grounding in future studies.

Second, we posit the need to study nuances in the profiles of victims and cyberstalkers with respect to behavioral (e.g., personality traits, attitude, motives) and functional parameters (e.g., online platform use, offline activities, costs associated with cyberstalking experience).

Third, we argue for the need to study victim-offender interactions and their influence on cyberstalking perpetration. Researchers should also adopt a temporal approach to understand the development of cyberstalking over time in terms of frequency and form of interaction—that is, both active (e.g., conversations, dialogue) and passive (e.g., ‘likes’ or sharing of online content such as pictures). It may also benefit scholars to know if such interactions affect the prevalence and intensity of cyberstalking.

Fourth, we believe future studies would benefit from investigating the influence of mediating or moderating variables on outcomes of cyberstalking. While two main forms of such variables that were derived from our SLR (i.e., victim-offender characteristics and internet/social media characteristics), we urge scholars to investigate other potential variables as well.

Next, scholars should consider investigating the effectiveness of intervening conditions, if any, that can be created by online platforms (e.g., policies for inappropriate online behavior), legal authorities, and civic stakeholders (communication norms, social support, and negative behavior toward cyberstalkers exhibited by parents, social groups educators, etc.).

Sixth, researchers may focus on refining the concept of cyberstalking, e.g., by refining pre-existing scales and considering specific roles of technological devices (e.g., smartphones) and platforms (especially social media) in inducing cyberstalking. Such investigations should consider the perspectives of stalkers, victims, as well as other civic stakeholders, in developing a holistic overview of cyberstalking. Lastly, scholars may attempt to advance current knowledge of victims’ behavioral (e.g., impacts on their psychological well-being, physiological functions, and social relationships) and functional responses (e.g., ceasing technology use, adopting stringent legal recourses, and managing financial costs of coping). Research should also be directed to investigate cyberstalkers’ reactions to victims’ responses—in particular, whether each potential form of response (formal and informal) has a deterring effect on stalking behaviors. Further, researchers should explicate if cyberstalkers exhibit other forms of deviant online behavior associated with the dark side of social media.

The proposed framework brings together some of the highlighted variables as well as gaps and emphasizes on the co-dependencies of the identified under-investigated associations, and factors. This framework is indicative and may be expanded by scholars to include more antecedents, indirect influences and consequences discussed in preceding sections.

6. Discussion and conclusion

The dynamic and evolving nature of technological environments has led to the emergence of multiple changes in communication norms and social interactions, with positive as well as negative ramifications on individuals. Cyberstalking is one such negative ramification, and

Figure 3. A research framework for future scholars
deviant behavior that can be categorized as a darker aspect of technology-enabled communication. An SLR was conducted following protocols recommended by previous studies to shed light on this phenomenon. Forty-nine empirical articles were identified and analyzed to develop a state-of-research profile and to present descriptive statistics on annual publication trends, the scope of investigations, top authors, leading publishers, methodologies, and sample characteristics (RQ1). Additionally, the analysis was used to explicate important themes from extant findings (RQ2), extant limitations and open research gaps (RQ3), and potential avenues for future research (RQ4).

Findings indicate that cyberstalking is a complex phenomenon with intricate ties to victims’ and stalkers’ personalities, technological platforms, as well as legal and social environments. Further, cyberstalking is rooted in and shares some similarities with its physical form, ‘offline’ stalking. To advance cyberstalking research, future research directions were proposed based on identified limitations and open research gaps. A research framework was proposed to assist scholars in promulgating thematic and methodological advancements that were indicated as critical by this SLR. The results have important implications for scholars and practitioners such as psychologists, therapists, and counsellors.

6.1. Theoretical implications

The present study contributes to scholarly knowledge through four key theoretical implications. Firstly, the primary contribution of this study rests in the identification of extant research gaps and viable agendas for future research. We also evaluate key under-represented associations as detailed in our proposed framework. Thus, by developing an organized précis of current information on cyberstalking, we provide a foundation for scholars to review extant intellectual boundaries and consider avenues for their expansion.

Secondly, the SLR highlights a dual (and thus more comprehensive) perspective on cyberstalking than previous studies by juxtaposing empirical evidence on victims with evidence on stalkers. Findings imply that the current academic understanding of cyberstalking is disproportionately oriented towards victims and needs to lay more emphasis on cyberstalkers in order to develop a more holistic and comprehensive understanding of this phenomenon.

Third, the dearth of empirical knowledge on the effects of internet/social media usage characteristics implies the need for refining our current understanding of cyberstalking in tandem with the evolution of technology that, by design, changes usage patterns. For example, key elements of smart devices, such as locational services provided by social media platforms including Instagram and Facebook, may facilitate cyberstalking. Thus, we must recognize that such effects will play a crucial role in cyberstalking perpetration in the future, implying that cyberstalking research may need to adopt a more comprehensive perspective on such technological factors.

Lastly, findings imply the need to advance cyberstalking research from a multi-disciplinary perspective by drawing from different schools of thought, e.g., information systems science, health psychology, and law. It is imperative that scholars consider these fields to make more nuanced empirical assessments of stalkers’ and victims’ cognitive, affective, and behavioral responses and/or actions. As the proliferation of technology is only slated to increase in the future, our findings also imply the need to focus on advocating for development of legal regulations to protect cyberstalking victims in consideration of their experience financial, psychological, and physiological strains.

6.2. Practical implications

We offer five practical implications through this SLR. First, the derived knowledge can guide mental health practitioners (e.g., psychologists, therapists, and counsellors) in helping cyberstalking victims to cope with their experiences and resultant trauma that diminishes their well-being. Practitioners should especially focus on the emotional and behavioral responses of cyberstalking victims to develop viable intervention strategies and coping mechanisms.

Secondly, findings imply that practitioners such as counsellors and therapists should focus their attention on assisting victims in coping not just with psychological trauma, but also detrimental financial, academic, and professional consequences that follow cyberstalking incidences. Our findings can assist practitioners in developing a more holistic view of cyberstalking; in refining existing and developing new strategies for its management, prevention, and reporting. Policymakers should also consider these consequences and adopt a holistic view of impairments suffered by victims while developing regulations to address cyberstalking. Such policymakers should especially consider the financial drain on victims and propose regulations for compensating them for the same.

Third, the findings may be used by counsellors, therapists, and policymakers to generate public awareness and disseminate information on cyberstalkers’ behavioral traits, along with prevalent characteristics and consequences of cyberstalking. This could assist individuals in safely using technology-enabled platforms, such as social media by identifying behavioral precursors displayed by a potential offender. It would also allow individuals to recognize cyberstalking and adopt protective measures pre-emptively.

Fourth, the study implies stakeholders (see 4.2.3) is a broader category than simply perpetrators and victims. We believe that parental and social group support can offer ample assistance to victims. Both mental health practitioners, and policymakers, should design informational content for disseminating information among parents and peers about the importance of offering support to victims, especially more vulnerable sections of the society (i.e., adolescents and young adults). Further, parents and educators could be encouraged to observe online activities of children and adolescents, and educate them about how other stakeholders are influenced due to cyberstalking. This could provide young and vulnerable individuals with guidance on safe online behaviors and potentially pre-empt cyberstalking.

Lastly, service providers of online platforms (e.g., social media), could introduce technical features that could warn individual users of a potential cyberstalking scenario. For example, individuals could be informed about excessive visits on their online profiles, and share basic information on profile visitors without impinging on users’ privacy, such as their name, and degree/ type of connection with the individual whose profile is being visited frequently. Further, platform users could be allowed to determine preferential activity and location-sharing, which would make it harder to track users’ movements and to glean information on their physical locations.

6.3. Social implications

The present study also raises significant implications for society in general; as even those who are not formally stakeholders in cyberstalking may be affected by cyberstalking and/or measures taken to prevent it. Firstly, we imply the consideration of cyberstalking as a societal problem, and need to adopt a stricter prosecutorial stance for reducing cyberstalking perpetration. While this may be done by refining existing laws, it is more important to encourage societal dissemination of information on cyberstalking. Stakeholders such as parents, peers, and educators may be encouraged to adopt social norms that may deter potential offenders and embolden victims (e.g., fear of being socially ostracized). Secondly, cyberstalking victims can suffer from severe negative consequences resulting not only from the incident, but from the social processes intended to prevent further damage. Members of legal and judicial professions may focus on easing reporting protocols and strengthening legal protection for such victims. Such refinements must be made in consideration of the continual evolution of technological environments, and ensure faster handling of reported cases. This would encourage more victims to come forth, which could consequently assist
Declaration of Competing Interest

The authors declare no potential conflicts of interest with respect to the research, authorship, and publication of this article.

Acknowledgements

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

References


Dhir, A., Yossatsorn, Y., Kaur, P., Chen, S., 2018. Online social media fatigue and psychological wellbeing—A study of compulsive use, fear of missing out, fatigue,


Puneet Kaur (DSc) is currently a postdoctoral researcher at Department of Psychosocial Science, University of Bergen, Norway. Her research appears in Journal of Retailing and Consumer Services, International Journal of Information Management, Computers in Human Behaviour, International Journal of Hospitality Management, Information Technology & People among others

Amandeep Dhir (DSc, PhD) is a Professor of Research Methods at University of Agder, Norway. He is also a visiting professor at Norwegian School of Hotel Management, University of Stavanger, Norway. His research appears in the Journal of Retailing and Consumer Services, International Journal of Information Management, Computers in Human Behaviour, Computers in Industry, International Journal of Hospitality Management, Journal of Cleaner Production, Food Quality and preferences, Appetite, Information Technology & People, Australasian Marketing Journal, Enterprise Information Systems among others

Anushree Tandon (PhD) is currently a researcher at Turku School of Economics, University of Turku, Finland. Her research appears in Computers in Human Behaviour, Computers in Industry, Food Quality and preferences, Appetite among others

Ebtesam Alzeiby (PhD) is currently an associate professor in Psychology Department, College of Education, Princess Nourah bint Abdulrahman University, Saudi Arabia. Her research interests include well-being, cyberpsychology, and psychological measures. Her research has appeared in the International Journal of Therapy and Rehabilitation, Child Care in Practice.

Abeer Ahmed Abohassan is currently a lecturer at the Social Planning Department, College of Social work, Princess Nourah bint Abdulrahman University, Saudi Arabia. Her research interests include online and offline stalking and social media.