Exploring the Effects of Personal and Situational Factors on Cyber Aggression

Hemamali Tennakoon1, Lucy Betts2, George Saridakis3, Chris Hand4, & Anil Chandrakumara5

1 Brunel Business School, Brunel University London, Uxbridge, United Kingdom
2 Department of Psychology, Nottingham Trent University, Nottingham, United Kingdom
3 Business School, University of Kent, Canterbury, United Kingdom
4 Business School, Kingston University, London, United Kingdom
5 School of Business, Faculty of Business & Law, University of Wollongong, Wollongong, Australia

Abstract

Antisocial behaviour by social media users has escalated, which in turn has created various socio-psychological implications for users and society at large. However, there is a paucity of empirical research on the concept of cyber aggression inclination (CAI) and its personal and situational antecedents in the context of social media. This study explores and measures the CAI of general social media users and examines the personal and situational factors affecting CAI. Data was collected using an online survey resulting in a sample of respondents who are active social media users. A total of 101 responses were received of which 71 were complete. Primary data was analysed using Partial Least Squares-Structural Equation Modelling (PLS-SEM) to test eight hypotheses. Findings suggest perceived anonymity, impulsive use of social media and subjective norms are correlated with and CAI. We could not find any conclusive evidence to suggest a significant association exerted by prior aggression victimisation, social pressure, and perceived incident severity on CAI. This paper makes original contributions to the field of cyberpsychology where a more specific form of antisocial behaviour has been studied in social media settings.

Keywords: social networking sites; cyber aggression; self-control; subjective norms; perceived anonymity

Editorial Record

First submission received: May 6, 2023
Revisions received: January 8, 2024
March 29, 2024
Accepted for publication: May 2, 2024
Editor in charge: Fabio Sticca

Introduction

The boundary between online and offline social spaces is blurring and offline behaviours are migrating to the online sphere (Ray & Kaushik, 2017). However, there is no regulation or gatekeeping in terms of which behaviours are acceptable and which are not (Awan & Zempi, 2016; J. Chan et al., 2016; Evolvi, 2018; Sessions, 2010; Sugarman & Willoughby, 2013; Udupa & Pohjonen, 2019). The concept of “online violence” has been studied in relation to general web users (Kaur et al., 2020; Kokkinos & Voulgaridou, 2017; Saridakis et al., 2016; Suzor et al., 2019; Zhong et al., 2020; Zhu et al., 2020). There is however room for further research around the concept of “cyber aggression”, particularly in the context of Social Networking Sites (SNS).

From extant literature, it emerges that “cyber aggression” is a broad term and comprises a wide range of antisocial online behaviours that include “bullying, harassment, stalking, abuse, assault or hostility, as well as violent behaviours such as ‘happy slapping, outing’ and ‘flaming’” (Grigg, 2010, p. 152). Aggressive behaviour is likely the
observable outcome of a trigger that leads to such behaviours. In support of this argument, DeWall and Chester (2016) posited that there is a distinction between an aggressive urge and aggressive action. There is the practical difficulty of measuring acts of aggression in real-time. Taking this into account, we base our definition on that suggested by Grigg (2010, p. 143) where Cyber Aggression Inclination (CAI) is defined as “intended harm and the use of technological devices” to act aggressively towards another individual in cyberspace.

This paper empirically examines the potential association between personal and situational factors as triggers of aggressive behaviour and cyber aggression inclination drawing on a number of theories. The General Theory of Crime (Gottfredson & Hirschi, 1990), for example, suggests that individual factors, such as self-control, are directly linked to criminal acts. The General Aggression Model (GAM; Anderson & Bushman, 2002) extends this view to include individual differences and situational factors that could affect the level of self-control. The later theory identifies personal factors such as attitudes (positive attitudes toward aggression), normative acceptance of aggression (norms), low self-control, and situational factors (e.g., anonymity) that are likely to influence aggressive behaviours (Anderson & Carnagey, 2004; DeWall et al., 2007, 2012; Gilbert & Daffern, 2011). Furthermore, Social Learning Theory suggests that individuals can mimic others’ aggressive behaviour through interpersonal observations and thus can internalise such behaviours (Bandura et al., 1963). Social Ecology Theory (Bronfenbrenner, 1977) further identifies personal and situational factors, supporting the argument that personal variables such as demographic traits (age, gender), past history (traditional bullying involvement), personality attributes (empathy, self-control), and external factors, such as peers, parents, mass media, cultural beliefs, etc., can lead to the perpetration of cyberbullying (Barlett, 2019).

Drawing on the theories outlined above and various recent studies (Dempsey et al., 2011; Heirman & Walrave, 2012; Lumsden, 2019; M. L. Williams & Pearson, 2016; Wright et al., 2018) we conclude that a two-dimensional approach that studies personal and situational factors as influencers of cyber aggression is appropriate. Particularly, we hypothesise associations between cyber aggression inclination and four personal factors: Higher empathy towards individuals; Low self-control; Prior cyber-aggression victimisation; and Negative normative beliefs about cyber aggression (subjective norms) and four situational factors: Social pressure; Intrinsic religiosity; Perception of anonymity; and perceived incident severity. The expected associations between cyber aggression and these factors are discussed in the next section where the foundations for the hypotheses are developed.

The contribution of this paper is to extend the existing literature, which mainly focuses on online violence towards general web users, by turning the research lens towards factors affecting cyber aggression inclination in online social media settings. This research develops and tests a theoretical model on cyber aggression inclination. The findings of this study will inform key stakeholders and practitioners (individual users, social media firms, government, law enforcement, and industry-based bodies) on the development of prevention and intervention procedures aimed at reducing cyber aggression impulses.

Hypotheses Development

Cyber aggression is an umbrella term that encompasses numerous types of negative behaviours online. These include activities such as flaming, online harassment, denigration, impersonation, outing and trickery, exclusion, cyber stalking, cyber threats, cyber bullying, etc. (Willard, 2007). In the context of SNS, the term cyber bullying has been used to refer to repeated aggressive behaviors on SNSs against targets who cannot defend themselves easily. (T. K. H. Chan et al., 2019, 2021). In this paper, we use the term “cyber-aggression” and adopt Grigg’s (2010, p. 152) definition as “intentional harm delivered by the use of electronic means to a person or a group of people irrespective of their age, who perceive(s) such acts as offensive, derogatory, harmful or unwanted”. There are many types of aggressive behaviours; they can be verbal, physical, and indirect (Card et al., 2008) and the nature of the aggressive behaviour depends on the intention of the aggressor (Galen et al., 1997). The level of aggression and the way in which aggression is shown can be context-specific.

Nevertheless, from a practical standpoint, it is challenging to measure participants’ levels of social aggression. Eraslan and Kukuoğlu (2019, p. 4) state that there is “no definite scientific definition for the concept of aggression. Not to mention the fact that the intention of an individual can be estimated but not exactly known”. Álvarez-García et al. (2016) also contend that acts of cyber aggression occur in virtual and often private environments, making them difficult to observe or measure. When respondents are asked if they behave aggressively, their self-reported responses may be biased and not always accurate. Therefore, in this research, we have focused on the propensity of a person to act aggressively, as measured by the variable Cyber Aggressive Inclination (CAI). We identify two
broad groups of predictors of CAI: personal factors and situational factors and identify four predictors in each: Virtual Empathy, Low Self Control, Subjective Norms and Prior Cyber Aggression Victimisation under personal factors and Social / Peer Pressure, Intrinsic Religiosity, Perceived Anonymity and Perceived Incident Severity under situational factors. These are introduced and developed below.

In previous studies, the below discussed factors have been researched independently but not collectively. Also, the associations tested in prior studies do not focus specifically on CAI, but on variations of aggressive and antisocial behaviours such as cyber bullying.

**Virtual Empathy and CAI**

According to Cuff et al. (2016), the term empathy is “not a well-defined notion” but can be understood as behaviour that involves comforting others (Caplan & Turner, 2007). Being empathetic means to be able to understand another person's emotional state (Cohen & Strayer, 1996). Previous studies have identified two types of empathy i.e., “affective empathy” (Van Noorden et al., 2017; Zych et al., 2019) and cognitive empathy (Caravita et al., 2010; Sutton et al., 1999). However, Garandeau et al. (2022, p. 515) argue that “findings on cognitive empathy...are less consistent”. Further, Gini et al. (2007), Jolliffe & Farrington (2006, 2011), Stavrinides et al. (2010) and Cheng et al. (2012) found no significant link between aggressive acts such as cyber-bullying and cognitive empathy. Therefore, we have used a more context-specific definition of empathy, namely “virtual empathy” (Carrier et al., 2015), defined as understanding others' emotions and sharing the emotional state of another person in computer-mediated communication or electronic communication environments, such as social media (Arató et al., 2020; Rudnicki et al., 2020).

Existing studies have used Social Ecology Theory to examine the association between (lack of) empathy and aggression. For instance, Steffgen et al. (2011) studied the relationship between an empathetic responsiveness and cyberbullying behaviour in adolescents. They find a negative association between the two variables in that cyberbullies are found to have less empathy towards others who are being victimised. Brewer and Kerslake (2015) draw a similar conclusion and find that low empathy is closely associated with antisocial behaviours, such as cyber aggression. Gini (2007) find that young people who have “affective empathy” are more likely to be involved in bullying intervention, while Mayberry and Espelage (2007) find that non-aggressive youth have higher empathy. Based on these findings, we argue that:

**H1:** Higher virtual empathy towards individuals is associated with lower cyber aggression inclination.

**Low Self-Control and CAI**

According to Duckworth and Kern (2011), self-control is a concept of interest to psychologists that is interchangeably used with other terms such as impulsivity, self-regulation, self-discipline, willpower, effortful control, ego strength, and inhibitory control (Evenden, 1999; White et al., 1994; Whiteside et al., 2005). S. Li and Nie (2023, p. 2) define self-control as “the ability to override or change one's inner responses, as well as to interrupt undesirable behavioral tendencies (such as impulses) and refrain from acting on them”. This definition suggests that self-control is a conscious act wherein the individual is actively motivated to regulate their behaviour. Additionally, Vohs and Baumeister (2004, p. 1) use the terms “self-control” and “self-regulation” interchangeably, defining them as the exercise of “control over oneself”. Drawing from the Social Cognitive Theory of self-regulation, self-control is also defined as the ability to regulate one's behaviours, thoughts, and emotions (Bandura, 1991). However, Howard’s (2011) Quadripartite Violence Typology (QVT) differentiates between two dimensions of self-control: impulsive versus premeditated, in relation to instrumental/premeditated and affective/impulsive violence. The current research primarily focuses on low self-control, indicating reduced self-regulation and increased impulsive behaviour.

In order to develop our hypotheses, we refer back to the General Aggression Model mentioned above which suggests an association between self-control and aggression. Anderson and Bushman (2002) suggest that a lack of self-control may be linked to aggressive tendencies in that an individual cannot sufficiently restrain impulses that are harmful to others. Vazsonyi et al. (2012) studied low self-control across 25 European countries and found that a deficit of self-control is associated with behavioural issues such as cyber-aggression. Further, DeWall et al. (2011) point out that the more self-control people have, the more likely it is that they will, before acting, consider the consequences of their actions towards others and choose to behave in a nonaggressive manner.
The findings above suggest that some researchers equate a lack of self-control with impulsivity, while others concentrate on outcome-oriented self-control, where individuals consciously regulate harmful behaviour. As previously mentioned, this research focuses on low self-control; therefore, we propose the following hypothesis:

**H2**: Low self-control is associated with higher cyber aggression inclination.

**Prior Cyber-Aggression Victimisation and CAI**

Cyber-aggression victimisation means prior exposure to intentional harm inflicted via information and communication technologies, such as being subjected to a form of aggressive behaviour online such as cyberbullying and cyberhate (Hawdon & Costello, 2020; Lewis et al., 2015; P. K. Smith et al., 2008; Wachs & Wright, 2018). As suggested by Hayes et al. (2020), experiencing aggression and victimisation can alter an individual’s personality. Existing evidence shows that being previously victimised by a cybercrime (such as cyber bullying) or offline bullying is associated with delinquent online behaviours. For example, P. K. Smith et al. (2008) find that victims of traditional bullying tend to become bullies themselves and bully others online.

There are many other studies showing a strong link between prior victimisation and the perpetration of cybercrime (Ang et al., 2011; Calvete et al., 2010; Dilsen, 2009; Hinduja & Patchin, 2007; Vandebosch & Van Cleemput, 2009; Ybarra & Mitchell, 2004; Ybarra et al., 2006). For example, Farrington et al. (2011) find that prior experience of bullying is associated with delinquency in later life. This is consistent with the findings from a study by Sigfusdottir et al. (2010) involving 15- and 16-year old adolescents in Iceland, where the researchers found that the strain created by victimisation is associated with anger, which in turn can lead to delinquency. Walters and Espelage (2018) find a strong association between victimisation and perpetration in a study involving adolescent/early adolescent children. The findings are consistent with the control model of criminal lifestyle development. Based on these findings, we argue that:

**H3**: Prior cyber-aggression victimisation is associated with higher cyber aggression inclination.

**Subjective Norms, Social Pressure and CAI**

Subjective norms and social pressure are separate concepts, and one is conceptualised as a personal factor and the other a situational factor. Despite this we discuss them together here as their effects on CAI have similar underlying mechanisms. Subjective norms can be defined as what an individual would perceive to be acceptable behaviour, depending on the attitudes and behaviours of people who are close or important to them (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1977; Rejón-Guardia et al., 2020; Venkatesh & Bala, 2008; Venkatesh & Davis, 2000). It can be argued that human aggression is reliant upon knowledge structures such as attitudes and beliefs (Anderson & Carnagey, 2004; Gilbert & Daffern, 2011), and aggressive knowledge structures are associated with aggressive behaviours (Allen et al., 2018). The potential relationship between normative beliefs and cyber aggression is complex and potentially different to those in the offline world. There is some evidence that people tend to behave more aggressively online when the social group norm was aggression (Rösner & Krämer, 2016). Further, although there was no direct effect of anonymity, people were more likely to conform to an aggressive social norm in an anonymous environment. Relatedly, students who experience classrooms where online aggression is considered normative (due to a higher frequency) are more likely to engage in aggressive online acts (Bullo & Schulz, 2022). However, the influence of the normative group did not extend to increases in an individual's level of aggression with changes in individual levels of aggression is the same irrespective of their peers’ reports of online aggression.

Whether behaviours are deemed appropriate or not is subjective and is partly determined by cultural factors (Lu et al., 2019). With reference to anti-social behaviours, Millie (2008, p. 379) argues that “what is regarded as anti-social is also determined by social and cultural norms of aesthetic acceptability”. Norms of the acceptability of aggressive behaviour are therefore context-specific and are influenced by the social actors present in a particular environment. For example, studies on aggressive language and bystander behaviour show that aggressive language originates in groups with similar normative assumptions and expectations (Parvaresh & Tayebi, 2018). Social groups tend to influence intra- and intergroup behaviours (Densley & Peterson, 2018; Ferreira et al., 2020). Hence it can argue that in-group/out-group behaviours are closely linked to peer pressure (Tafel et al., 1971).

Aderibigbe and Ocholla (2020, p. 5) argue that “subjective norms are an important attribute when determining ethical intention with respect to cyber technology” and state that “reference groups...have influential roles to play
in determining ethical and unethical cyber behaviour”. These reference groups could be family as in Subjective Norms, or social peers resulting per pressure. Drawing on prior studies (Aderbigbe & Ocholla, 2020; Richetin et al., 2011; Setijanto et al., 2019), Subjective Norms and Social Pressure are treated as separate variables in this study. Both norms and social pressure are collective expectations and in certain societal settings, individuals may be influenced or compelled to adhere to certain norms (Theriault et al., 2021). Further, Barlett (2023, p. 6) argue that “cyberbullying perpetration is a learned social behavior” and can be explained using the social learning theory. Hence, we suggest the following two hypotheses:

**H4:** Negative normative beliefs about cyber aggression are associated with lower cyber aggression inclination.

**H5:** Increased social pressure is associated with lower cyber aggression inclination.

*Intrinsic Religiosity and Cyber Aggression Inclination*

Religiosity is a widely studied concept in psychology, personality, mental health, ethics, and marketing settings (Abeyta & Blake, 2020; Mosquesiro et al., 2015; Pirutinsky et al., 2011; Uysal & Okumuş, 2019). It is a complex construct with multiple definitions (Abdel-Khalek, 2019). Allport and Ross (1967) introduced two dimensions of religiosity: intrinsic and extrinsic. In this paper, we follow Mendolia et al. (2019, p. 2) who argued that “intrinsic religiosity is a better indicator of the role that religion per se plays in an individual’s decisions and attitudes”. To this end, intrinsic religiosity is defined as the tendency of a person to find their motivation in their religion (Allport & Ross, 1967) and intentionally “integrate religion into one’s life” (Pirutinsky et al., 2011).

Several papers find an association between intrinsic religiosity and risky behaviour. It has been argued that religiosity provides individuals with a reference framework of what behaviours are risky/acceptable and how to control and regulate one’s behaviours (Hungerman, 2014; McCullough & Willoughby, 2009; Mellor & Freeborn, 2011). Some suggest that religious commitment leads to positive social interactions (e.g., Hardy et al., 2012). Conversely, Golec de Zavala et al. (2012) identified intrinsic religiosity as a predictor of intergroup hostility. Further, in a study involving adolescents in religious and secular schools in Israel, it was found that “cyber-bullying was more common among secular students than religious students” (Tesler et al., 2019). Here, we propose to test the following hypothesis:

**H6:** Intrinsic religiosity is associated with lower cyber aggression inclination.

*Perceived Anonymity and CAI*

Hite et al. (2014, p. 23) defined anonymity “as the state of being unidentified or unknown”. In communications and information systems research, anonymity is further described as “environmental, content-based, and procedural” (Gavish & Gerdes, 1998, p. 297) and incorporates non-identifiability (Marx, 1999; Wallace, 1999). However, there is debate among scholars regarding the distinction between “perception of anonymity” and “actual anonymity” (Gavish & Gerdes, 1998; Hite et al., 2014; C. R. Scott, 1998). For example, Mishna et al. (2009) find that anonymity is considered integral to cyber bullying, but that participants are uncertain as to “whether the Internet and other communication technologies provide actual or perceived anonymity for the aggressor”. Choi et al. (2016) tested the concept “degree of anonymity perception” by classifying it into social anonymity, visual anonymity, definitive anonymity, and location anonymity. Results revealed that online community users with a high degree of visual and location anonymity are more likely to post malicious messages. As a construct, anonymity has also been studied as two broad categories in online communication research: technical anonymity and social anonymity. Technical anonymity refers to the removal of personally identifiable information about a person whereas social anonymity refers to the individual’s perception of identifiability due to the lack of personal cues (Hayne & Rice, 1997). Hence, Christopherson (2007, p. 3040) argues that “it may not be the case that one is truly anonymous in a social context, but the individual perceives him or herself to be anonymous to others”.

Studies show that varying levels of perceptions about anonymity are found to be correlated with different levels of behaviours (Piazza & Bering, 2008). In online settings, perceived anonymity is found to be negatively associated with self-awareness and self-control, which in turn results in deindividuation (Hilvert-Bruce & Neill, 2020; Lowry et al., 2016; Suler, 2004; Zimbardo, 1969). The deindividuation effect has also been found to reduce awareness of oneself and reduce the impact of social norms, leading to a disinhibition effect and influencing aggressive behaviours (Diener, 1976; Dooley et al., 2009; Festinger et al., 1952; Nakano et al., 2016; Perfumi, 2020; Rogers & Prentice-Dunn, 1981; Suler, 2004; Vranjes et al., 2020; Wright, 2013, 2014a, 2014b). Barlett and Gentile (2012)
provide more supporting evidence to suggest that in first time youth cyberattacks, the individuals learn to perceive themselves as more anonymous online and this perceived anonymity could lead to perceived cyber-attacks and cyber bullying. Based on these findings, we suggest that:

**H7:** Higher perception of anonymity is associated with higher cyber aggression inclination.

**Perceived Incident Severity and CAI**

Studies show that aggressive acts online can have a more severe impact on individuals than their offline equivalents (e.g., cyber bullying versus traditional bullying; Dredge et al., 2014; Gül et al., 2019; Wang et al., 2019). Some argue that the severity of incidents in online behaviour can be viewed through the perception of either the target (victim) or the bystanders (e.g., Macaulay et al., 2019). From a bystander's perspective, the decision to assist a victim of cyberbullying depends on the perceived severity of the incident (Bastaensens et al., 2014; Roman et al., 2020). For instance, bystanders may perceive a situation as more severe if it includes threats of physical assault (Allison & Bussey, 2016). Studies involving young people have shown that bystanders assess the likely impact of different types of bullying on victims and that the severity of an incident influences their willingness to intervene (Bastaensens et al., 2014; Cappadocia et al., 2012; Chen et al., 2015; Macaulay et al., 2019; Obermaier et al., 2016; K. R. Williams & Guerra, 2007). A recent study on celebrity abuse on Twitter found that “the volume of abuse influenced both attributed blame and perceived incident severity” (G. G. Scott et al., 2020, p. 23).

The severity of an incident can also be viewed from the victim's perspective. For example, Rivers & Noret (2010) identified several forms of cyberbullying (e.g., verbal abuse, uploading images onto websites, distributing images via mobile phones) and argued that the severity of the incident varies with the nature of the bullying experienced by the victim. G. G. Scott et al. (2020) suggest that interpretations of abusive incidents will differ among individuals. In other words, certain behaviours may be deemed less severe by some, potentially increasing their inclination toward aggression. Therefore, in the current research, we employ the concept of “perceived incident severity” to denote an individual's assessment of the likely impact of an aggressive act on another person (Chen et al., 2015; Kwan & Skoric, 2013; Vandebosch & Van Cleemput, 2009). The individual evaluating the situation and judging the incident's severity may be either the victim or a bystander.

Therefore, we propose to test the following hypothesis:

**H8:** High perceived incident severity is associated with lower cyber aggression inclination.

**Methods**

**Data Collection**

The study population consists of social media users on the World wide web. In the absence of a sampling frame, the current research uses a non-probability convenience sampling. The sampling design of the current research is drawn from the works of (Brickman Bhutta, 2012; Göritz et al., 2012; Kapp et al., 2013; T. W. Smith, 2013) and closely follows the approach employed by Brickman Bhutta (2012) in similar web-based research. The survey instrument was developed using Qualtrics survey software. Prior to administering the survey, ethics board approval was obtained from the universities of the principal investigators; all participants were fully informed about the general scope of the study, informed consent was collected from every participant, and no remuneration was given for participation.

Given that the active social media user is a parameter of interest for this research, the online survey was posted on the SNS Facebook and LinkedIn. Over a period of fifteen months (November 2019–February 2021), we received 101 responses (respondents mainly from the UK and Sri Lanka with few from Spain, Germany, the USA, Canada, France, Finland, Singapore, Bangladesh, and Thailand). The response rate of the study was low because the topic was sensitive, and participants may have been reluctant to share information through the online survey. We acknowledge the small sample size and the length of time the survey was available. However, limiting the timeframe as we did is appropriate because of the rapidly evolving nature of online spaces and that online behaviour changed during the pandemic (Petrović et al., 2022). Data cleaning involved removal of any partial completed questionnaires from the dataset. This led to a diminished dataset of 71 responses, which was analysed using SPSS and SmartPLS 3. The measures used in this study are based on measures previously validated in the
published literature. Table 1 provides a summary of the measures used and sources from which the scale items were obtained.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Source</th>
<th>Measures</th>
<th>Scale used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual empathy</td>
<td>Carré et al. (2013)</td>
<td>EMP_2: I don't become sad when I see other people crying.</td>
<td>Strongly disagree (1)-Strongly agree (5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EMP_3: Other people's feeling don't bother me at all.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EMP_6: Seeing a person who has been angered has no effect on my feelings.</td>
<td></td>
</tr>
<tr>
<td>(low) Self-control</td>
<td>Grasmick et al. (1993)</td>
<td>SELFC_5: I wish I had more self-discipline when in am using SNS.</td>
<td>Not at all like me (1)-Very much like me (5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SELFC_7: Sometimes I can't stop myself from doing something, even if I</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>know it is wrong.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SELFC_8: I often act without thinking through all the alternatives.</td>
<td></td>
</tr>
<tr>
<td>Cyber-Aggression Victimisation</td>
<td>Williams and Mattson (2006)</td>
<td>PRIOR_VIC_1: How often in the last few months, have you had anyone</td>
<td>Very often (1)-Not at all often (4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>telling lies or making fun of you on SNS?</td>
<td></td>
</tr>
<tr>
<td>Social pressure</td>
<td>Buhrmeister and Furman (2008)</td>
<td>SOCIALP_1: How often do your friends push you to do things on SNS that</td>
<td>Very often (1)-Not at all often (4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>you don't want to do?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOCIALP_2: How often do your friends try to get you to do things on SNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>that you don't like?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOCIALP_3: How often do your friends pressure you to do the things they</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>want on SNS?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOCIALP_4: How often do you feel obliged to share certain posts on SNS,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>even though you do not want to yourself?</td>
<td></td>
</tr>
<tr>
<td>Subjective Norms</td>
<td>Richetin et al. (2011)</td>
<td>NORMS_1: People who are important to me think it is ok to use SNS to</td>
<td>Not at all likely (1)-Very likely (5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>express my views against someone/a group when I am angry with them.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NORMS_2: People who are important to me would approve of me using SNS to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>express my views against someone/a group when I am angry with them.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NORMS_3: People who are important to me would be very happy if I use</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>express my views against someone/a group when I am angry with them.</td>
<td></td>
</tr>
<tr>
<td>Intrinsic Religiosity</td>
<td>Gorsuch and McPherson (1989)</td>
<td>RELIG_2: Although I am religious, I don't make decisions based on my</td>
<td>Strongly disagree (1)-Strongly agree (5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>religious beliefs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RELIG_3: Although I believe in my religion, many other things are more</td>
<td>Very likely (1)-Not at all likely (4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>important in life.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RELIG_4: How I treat others are not based on my personal religious beliefs.</td>
<td></td>
</tr>
<tr>
<td>Perceived Anonymity</td>
<td>Hite et al. (2014)</td>
<td>ANON_3: I am easily identified as an individual by others.</td>
<td>Very likely (1)-Not at all likely (4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ANON_4: Others are likely to know who I am.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ANON_5: My personal identity is known to.</td>
<td></td>
</tr>
<tr>
<td>Perceived Incident Severity</td>
<td>Pabian et al. (2015) and 4 new</td>
<td>ISEV_1: Damaging someone else's reputation by spreading rumours about</td>
<td>Not a severe incident (1)-Very severe incident (5)</td>
</tr>
<tr>
<td></td>
<td>items</td>
<td>them on SNS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISEV_2: Liking and commenting on posts on SNS that are intended to bully</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a person/group (e.g., religious group).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISEV_3: Resharing a post containing hateful comments about a certain</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>person/group (e.g., religious group) on SNS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISEV_4: Insulting another person/group (e.g., religious group) publicly</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>on SNS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISEV_5: Posting embarrassing photos or videos of someone else on SNS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISEV_6: Deliberately excluding someone from an online social group to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>make him/her feel excluded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISEV_7: Sending threatening messages/reactions to someone on SNS.</td>
<td></td>
</tr>
<tr>
<td>Cyber Aggression Inclination</td>
<td>Buss and Perry (1992), Bryant</td>
<td>AGG_INC_1: I often use SNS to express my views against someone/a group</td>
<td>Strongly disagree (1)-Strongly agree (5)</td>
</tr>
<tr>
<td></td>
<td>and Smith (2001)</td>
<td>that I don't like.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AGG_INC_2: I often create posts on SNS that are against people/groups I</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>don't like.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AGG_INC_3: I often reshare posts condemning a person/group I don't like.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AGG_INC_4: I often comment on posts I see on SNS that are about people/groups that I don't like.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 1. Variable Measures.**
Dependent and Independent Variables

All five items for measuring the dependent variable “cyber aggression inclination” were developed using Buss and Perry (1992) and Bryant and Smith (2001). When tested, the items showed high reliability and all items were retained in the final instrument. The items for the independent variables were developed as follows:

The seven items for “virtual empathy” were derived from Carré et al. (2013). Initial testing identified a very low Average Variance Extracted. Further investigation revealed that one item (item 7) loaded onto a factor on its own. Although the construct was expected to be unidimensional, the remaining items loaded onto two factors. Items 2, 3 and 6 loaded onto one which we term “unemotional”. Items 4 and 5 loaded onto a second factor we label as empathy; item 1 was dropped due to a loading below 0.7. Self-control had eight items sourced from Grasmick et al. (1993) measured on a scale Not at all like me (1)–Very much like me (5). A similar issue emerged where a scale expected to be unidimensional produced two factors. Items 1, 2, 3 and 4 loaded onto one factor which captured perceived self-control whilst items 5, 6, 7, 8 loaded onto a separate factor which we label impulsive SNS use. Cyber-Aggression Victimisation is measured using a single item asking if the respondent had experienced being made fun of or lied about. The “subjective norms” construct was measured using three items, all of which were retained. Similarly, the four items sourced from Buhrmester and Furman (2008) to measure social pressure were found to have high reliability and were retained for the final questionnaire Intrinsic religiosity was measured using four items. One (item 1) was dropped because of a low loading. The other three items were reverse coded so that a higher score reflects a greater degree of religiosity. “Perceived anonymity” was measured using five items. Finally, Perceived Incident Severity was measured using 7 items. Three of these items were based on Pabian et al. (2015). We also added four new items (i.e., items 1–4) to broaden the scope of the types cyber bullying scenarios that would be deemed as severe to include spreading rumours about someone and liking or sharing bullying or hurtful comments. When all seven items were used, the reliability measures, Cronbach’s alpha and Composite Reliability, were very high (above .97). Items 3 and 4 were found to be strongly correlated so item 3 was dropped as a redundant item.

In Table 2 we present the respondents’ demographic information. Majority of the respondents (69%) were female and 30% were male respondents. 97% of the respondents were educated at University degree level. The distribution based on job status shows that 62% of the sample were employed and 25% unemployed. Marital status shows 63% of respondents as single and 37% as married. The majority of respondents are aged under 50, with just over half (52%) aged 18–28.

<table>
<thead>
<tr>
<th>Measure</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>30</td>
</tr>
<tr>
<td>Female</td>
<td>69</td>
</tr>
<tr>
<td>Non-binary</td>
<td>1</td>
</tr>
<tr>
<td>Level of education</td>
<td></td>
</tr>
<tr>
<td>Secondary education</td>
<td>3</td>
</tr>
<tr>
<td>University degree</td>
<td>97</td>
</tr>
<tr>
<td>Current job status</td>
<td></td>
</tr>
<tr>
<td>Self-employed</td>
<td>11</td>
</tr>
<tr>
<td>Employed</td>
<td>62</td>
</tr>
<tr>
<td>Unemployed</td>
<td>25</td>
</tr>
<tr>
<td>Prefer not to say</td>
<td>1</td>
</tr>
<tr>
<td>Marital status</td>
<td></td>
</tr>
<tr>
<td>Single</td>
<td>63</td>
</tr>
<tr>
<td>Married</td>
<td>37</td>
</tr>
<tr>
<td>Age</td>
<td></td>
</tr>
<tr>
<td>18–28</td>
<td>52</td>
</tr>
<tr>
<td>29–39</td>
<td>30</td>
</tr>
<tr>
<td>40–49</td>
<td>13</td>
</tr>
<tr>
<td>50–59</td>
<td>0</td>
</tr>
<tr>
<td>60–69</td>
<td>1</td>
</tr>
<tr>
<td>Over 69</td>
<td>4</td>
</tr>
<tr>
<td>Prefer not to say</td>
<td></td>
</tr>
</tbody>
</table>
**Empirical Approach**

We use Partial Least Squares-Structural Equation Modelling (PLS-SEM) in the assessment of measurement, structural models, and hypotheses testing. PLS-SEM does not require a normal distribution of data and can accommodate smaller sample sizes.

The first step in PLS-SEM assessment involves an examination of the measures of item reliability, construct reliability, and convergent validity, which are assessed using the criteria discussed in Hair et al. (2011), Bagozzi and Yi (2012). As discussed above, several items showed low loadings and they were removed to improve the overall reliability and validity of the measurement model. This was assessed using the criteria discussed in Hair et al. (2011) and Bagozzi and Yi (2012). Table 3 shows the test statistics for items that remained. All of the constructs demonstrated satisfactory reliability (assessed using Cronbach's Alpha and Composite Reliability) and convergent validity (all loadings are greater than 0.7 and all Average Variance Extracted values are above 0.5). Discriminant validity is then assessed using the square root of average variance extracted (AVE) values and item correlations. Table 4 shows the discriminant validity where the values in bold along the diagonal are the square root of the AVE of the latent variables. Off-diagonal elements are the correlation values between the variables. Discriminant validity is adequately demonstrated in this study since the diagonal elements are larger than the off-diagonal elements in the corresponding row and column (Duarte & Raposo, 2010; Hair et al., 2011).

We also investigated the degree of skewness and kurtosis for the constructs. Both skewness and excess kurtosis values lay outside the acceptable range of -2 to 2 for Cyber Aggression Inclination (skewness = 2.184 and excess kurtosis = 5.964) as do excess kurtosis values for Cyber Aggression Victimisation's (5.424) and for Unemotional (2.528). All other skewness and kurtosis values lay within the -2 to 2 range.
<table>
<thead>
<tr>
<th>Constructs</th>
<th>Items</th>
<th>Loadings</th>
<th>AVE</th>
<th>Composite Reliability</th>
<th>Cronbach's Alpha</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior aggression victimisation</td>
<td>PRIOR_VIC_1</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td></td>
<td>AGG_INC_1</td>
<td>.867</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AGG_INC_2</td>
<td>.916</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber aggression inclination</td>
<td>AGG_INC_3</td>
<td>.919</td>
<td>.783</td>
<td>.947</td>
<td>.930</td>
</tr>
<tr>
<td></td>
<td>AGG_INC_4</td>
<td>.871</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AGG_INC_5</td>
<td>.849</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ANON_3</td>
<td>.847</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perceived anonymity</td>
<td>ANON_4</td>
<td>.936</td>
<td>.815</td>
<td>.929</td>
<td>.886</td>
</tr>
<tr>
<td></td>
<td>ANON_5</td>
<td>.922</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EMP_2</td>
<td>.860</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unemotional</td>
<td>EMP_3</td>
<td>.759</td>
<td>.741</td>
<td>.852</td>
<td>.659</td>
</tr>
<tr>
<td></td>
<td>EMP_6</td>
<td>.813</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EMP_4</td>
<td>.830</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Empathy</td>
<td>EMP_5</td>
<td>.870</td>
<td>.723</td>
<td>.839</td>
<td>.618</td>
</tr>
<tr>
<td></td>
<td>ISEV_1</td>
<td>.957</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISEV_2</td>
<td>.903</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISEV_3</td>
<td>.937</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perceived incident severity</td>
<td>ISEV_5</td>
<td>.930</td>
<td>.856</td>
<td>.973</td>
<td>.968</td>
</tr>
<tr>
<td></td>
<td>ISEV_6</td>
<td>.887</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISEV_7</td>
<td>.946</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subjective norms</td>
<td>NORMS_1</td>
<td>.870</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NORMS_2</td>
<td>.922</td>
<td>.823</td>
<td>.933</td>
<td>.892</td>
</tr>
<tr>
<td></td>
<td>NORMS_3</td>
<td>.929</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RELIG_2</td>
<td>.855</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrinsic religiosity</td>
<td>RELIG_3</td>
<td>.964</td>
<td>.707</td>
<td>.876</td>
<td>.821</td>
</tr>
<tr>
<td></td>
<td>RELIG_4</td>
<td>.678</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SELFC_1</td>
<td>.665</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perceived self-control</td>
<td>SELFC_2</td>
<td>.844</td>
<td>.627</td>
<td>.869</td>
<td>.809</td>
</tr>
<tr>
<td></td>
<td>SELFC_3</td>
<td>.771</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SELFC_4</td>
<td>.87</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SELFC_5</td>
<td>.695</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Impulsive SNS use</td>
<td>SELFC_7</td>
<td>.864</td>
<td>.597</td>
<td>.853</td>
<td>.787</td>
</tr>
<tr>
<td></td>
<td>SELFC_8</td>
<td>.880</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SOCIALP_1</td>
<td>.890</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social pressure</td>
<td>SOCIALP_2</td>
<td>.890</td>
<td>.659</td>
<td>.885</td>
<td>.838</td>
</tr>
<tr>
<td></td>
<td>SOCIALP_3</td>
<td>.720</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SOCIALP_4</td>
<td>.740</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 4. Discriminant Validity.

<table>
<thead>
<tr>
<th>Pathway</th>
<th>Path coefficient</th>
<th>Standard deviation</th>
<th>t statistic</th>
<th>p value</th>
<th>f-square</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Cyber Aggression Inclination</td>
<td>.885</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Cyber Aggression Victimisation</td>
<td>−.039</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Empathy</td>
<td>.258</td>
<td>.099</td>
<td>.85</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Intrinsic Religiosity</td>
<td>.199</td>
<td>.326</td>
<td>.229</td>
<td>.841</td>
<td></td>
</tr>
<tr>
<td>5 Impulsive SNS use</td>
<td>.508</td>
<td>−.103</td>
<td>.221</td>
<td>.084</td>
<td>.773</td>
</tr>
<tr>
<td>6 Perceived Anonymity</td>
<td>.601</td>
<td>−.104</td>
<td>.368</td>
<td>.052</td>
<td>.374</td>
</tr>
<tr>
<td>7 Perceived Incident Severity</td>
<td>.151</td>
<td>−.023</td>
<td>.046</td>
<td>.033</td>
<td>.069</td>
</tr>
<tr>
<td>8 Perceived Self Control</td>
<td>−.078</td>
<td>−.039</td>
<td>−.036</td>
<td>−.112</td>
<td>−.158</td>
</tr>
<tr>
<td>9 Subjective Norms</td>
<td>.617</td>
<td>−.011</td>
<td>.153</td>
<td>.176</td>
<td>.36</td>
</tr>
<tr>
<td>10 Social Pressure</td>
<td>.226</td>
<td>.301</td>
<td>.189</td>
<td>.329</td>
<td>.004</td>
</tr>
<tr>
<td>11 Unemotional</td>
<td>.409</td>
<td>.25</td>
<td>.043</td>
<td>.177</td>
<td>.25</td>
</tr>
</tbody>
</table>

Note. Elements in bold are the square root of the AVE for that construct; other elements are correlation coefficients.

Results

Structural Model Assessment and Hypotheses Testing

SmartPLS 4 was used to assess the structural model. This involved testing the hypothesised relationships among the latent constructs and evaluating the coefficient of determination ($R^2$). The $R^2$ suggests that the independent constructs explain 59% of the variation in CAI. We then use a bootstrapping re-sampling procedure to assess the significance of the path estimates for hypotheses testing (Hair et al., 2011; Tenenhaus et al., 2005). PLS-SEM is suitable for the small sample size of this study because it is capable of achieving high statistical power (Reinartz et al., 2009; Sosik et al., 2009). To test the significance of the path coefficients, one-tailed hypothesis tests are adopted.

The path estimates are presented in Table 5. The results support the hypothesised association between unemotionality and CAI, however, empathy is not significantly associated with CAI (H1), impulsive SNS use and CAI, but not between self-control and CAI (H2), subjective norms and CAI (H4), and lastly perceived anonymity and CAI (H7).

Table 5. Path Coefficients, Significance Tests and Effect Sizes.

<table>
<thead>
<tr>
<th>Pathway</th>
<th>Path coefficient</th>
<th>Standard deviation</th>
<th>t statistic</th>
<th>p value</th>
<th>f-square</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1 Emathpy → Aggression inclination</td>
<td>.038</td>
<td>.086</td>
<td>0.44</td>
<td>.330</td>
<td>.003</td>
</tr>
<tr>
<td>Unemotional → Aggression inclination</td>
<td>.215</td>
<td>.127</td>
<td>1.69</td>
<td>.046</td>
<td>.071</td>
</tr>
<tr>
<td>H2 Perceived Self Control → Aggression inclination</td>
<td>−.083</td>
<td>.128</td>
<td>0.653</td>
<td>.257</td>
<td>.013</td>
</tr>
<tr>
<td>Impulsive SNS use → Aggression inclination</td>
<td>.228</td>
<td>.109</td>
<td>2.086</td>
<td>.019</td>
<td>.095</td>
</tr>
<tr>
<td>H3 Prior aggression victimisation → Aggression inclination</td>
<td>−.122</td>
<td>.117</td>
<td>1.045</td>
<td>.148</td>
<td>.026</td>
</tr>
<tr>
<td>H4 Subjective Norm → Aggression inclination</td>
<td>.303</td>
<td>.121</td>
<td>2.507</td>
<td>.006</td>
<td>.125</td>
</tr>
<tr>
<td>H5 Social Pressure → Aggression inclination</td>
<td>.203</td>
<td>.174</td>
<td>1.166</td>
<td>.122</td>
<td>.073</td>
</tr>
<tr>
<td>H6 Intrinsic Religiosity → Aggression inclination</td>
<td>.039</td>
<td>.135</td>
<td>0.293</td>
<td>.385</td>
<td>.003</td>
</tr>
<tr>
<td>H7 Perceived Anonymity → Aggression inclination</td>
<td>.226</td>
<td>.112</td>
<td>2.028</td>
<td>.021</td>
<td>.07</td>
</tr>
<tr>
<td>Perceived Incident Severity → Aggression inclination</td>
<td>.024</td>
<td>.128</td>
<td>0.188</td>
<td>.425</td>
<td>.001</td>
</tr>
</tbody>
</table>

Note. Standard deviations are bootstrapped using 5,000 subsamples.
Factors That Are Found to Be Significantly Associated With Cyber Aggression Inclination

The analysis of the data confirmed the hypothesised relationships between one of our two measures of virtual empathy and CAI (H1), one of our two measures of self-control and CAI (H2), subjective norms and CAI (H4), and between perceived anonymity and CAI (H7). For example, Fraser et al. (2012) find an association between low empathetic concern lower prosocial behaviour toward strangers in the context of violent video gaming. However, in a similar context, Lemercier-Dugarin et al. (2021) find that gamers with high levels of empathy are “less likely to be toxic”. Further findings by Marín-López et al. (2020) find no association between online empathy and deviate behaviours such as cyberbullying. Our results show an indifference to others’ emotions is associated with CAI whilst empathy has no effect on it. As such our findings support those reported by Marín-López et al. (2020) and by Fraser et al. (2012).

In support of H2, it was found that low self-control, in terms of impulsive use of SNS is positively associated with cyber aggression inclination. Our measure of perceived self-control however shows no association with CAI. In another study involving students, those with high self-control show positive regulation of behaviour and avoid acts of violence against their friends (Cantone et al., 2015). In the context of online social networking and ICT-led communication, an absence of self-control is found to increase cyber-aggression (Runions, 2013). Individual differences in self-control also seem to contribute to proclivities for aggression and antisocial behaviour (Gottfredson & Hirschi, 1990). Further, Lee et al. (2013, p. 736) identify self-control as a “constructs related to controlling one’s actions” and argue that “self-control decreases virtual aggression”. In a more recent study, Peker and Yıldız (2021, p. 40) found that self-control could mediate the relationship between the aggressive behaviors and the cyber bullying behaviors which suggests room for future research in testing the mediating effect of self-control on CAI.

Evidence supporting the findings of H4 show that normative beliefs are associated with cyber aggression. Studies show that individuals who approve of classmates/peers who are involved in cyberbullying are more likely to become cyberbullying perpetrators (Doane et al., 2014; Festl et al., 2015; Sasson & Mesch, 2014). Further, in adolescent studies, subjective norms were identified as a potentially strong predictor of the intention to engage in cyberbullying behaviour (Heirman & Walrave, 2012; K. R. Williams & Guerra, 2007). In online gaming environments, normative beliefs significantly predict cyberaggression (Hilvert-Bruce & Neil, 2020). In contrast, Festl (2016) found that subjective norms do not have a significant role to play in the individual perpetration of bullying.

Our findings also show that perceived anonymity and CAI are associated (H7) and this is supported by prior research. In social media research there is evidence to suggest that users can become more verbally aggressive in an anonymous environment (Rösner & Krämer, 2016). Another study reveals that “aggressor-perceived anonymity is an important risk factor for later cyberbullying behaviour” (Barlett et al., 2016, p. 171). Several other studies support our findings that identify anonymity as a contributor to online aggression because it allows individuals to act in a disinhibited way (Herring, 1999; Joinson, 2007; Q. Li, 2007; Tanis & Postmes, 2007).

Factors That Are Not Significantly Associated With Cyber Aggression Inclination

The remaining hypotheses (H3, H5, H6 and H8) are not supported by the data. There is evidence from past research which suggest that a history of past abuse and victimisation could be associated with abusive behaviour and victimization of others in adulthood (Firoozabadi, 2020). This is in contrast to our finding for (H3) which shows no association between prior aggression victimisation and CAI. The above research involved reviewing of patients referred to a private outpatient clinic. The contextual differences and the self-report nature of data we obtained for our study could account for the lack of support for H3 in the current study.
Moreover, H5 was also not supported. In previous research, it was argued that influence of others on cyberbullying could depend on the priorities of a certain group and the unity/coherence of the group (Dang & Liu, 2020). This is further supported by Bleize et al. (2021) where it is argued that conformity to peer behaviour and social identification could be associated with aggression in adolescent. In the current study, we were not studying specific groups (e.g., peer groups, adolescents, gender groupings of respondents, cultural or other social grouping) and the respondents were reporting their individual behaviours rather than in the context of a specific group. This could account for the findings for H5. This might also explain why similar sized path coefficients attached to other constructs are significant. There certainly seems to be more variation (as captured by the standard deviation) for this construct, which in turn reduces the value of the $t$-statistic.

In H6 our expectation was that intrinsic religiosity would have a negative effect on CAI, drawing on earlier findings that religiosity can regulate behaviour. Instead, we find no significant association between them. However, in this study supports Bhargava and Kaura’s (2020) finding that religiosity is not significantly associated with aggression.

We also explored the association between perceived incident severity and CAI in H8 which was not supported. This may reflect the difficulties of measuring perceived severity in a survey study rather than a scenario-based study. Moreover, the current research used the concept of “perceived incident severity” to denote an aggressor’s evaluation of the likely impact of an aggressive act on a victim. This is a personal evaluation that an aggressor would perform subjectively and from one individual to another, this assessment could vary. For instance, what may be considered as a “severe” incident by one person may be perceived as no so by another. Therefore, future research should consider adopting a scenario based or vignette-based approach with multi-level modelling as they enable researchers to collect rich data on topics that present challenges when trying to study them directly (Baguley et al., 2022).

To extend our analysis further we apply Importance-Performance Map Analysis (IPMA) to our PLS results (Ringle & Sarstedt, 2016, provide an overview). The strength of relationship between constructs is captured by the magnitude of the coefficient. In IPMA this is termed importance and is captured by unstandardized total effects of a construct which is rescaled to lie between 0 and 100. IPMA additionally considers the average latent score (performance). From this, researchers can identify constructs which have a strong relationship with the target construct but also have relatively low or high performance (relatively low or high average scores). A construct with high importance but low performance could be a target for intervention. The high importance shows a greater effect of a change in a predecessor construct on the target variable. Low/high performance indicates that there is scope to increase/decrease the value of that predecessor construct.

By convention, IPMA results are presented as a plot of Importance (on the X axes) against Performance (on the Y axis). Importance and Performance values were calculated using SmartPLS4. The map resulting from IPMA analysis on our data is shown in figure 1 below.

**Figure 1. Importance-Performance Map Analysis.**
The four constructs with significant pathways: perceived anonymity, Impulsive SNS use, Subjective Norms and Unemotional; all appear on the right-hand side of the map. They also all have lower performance than most other constructs (indicating that responses tend towards the lower end of the scale). Of these, Subjective Norms and Perceived Anonymity would be more easily influenced than impulsive use or being unemotional. The Subjective Norm items are phrased so that lower performance is the desirable outcome. Lower performance signifies that posting view when angry would not be approved of by those important to the respondent. As such there is less scope to influence subjective norms further. A similar argument holds for perceived anonymity.

Social Pressure seems to stand out in the map. Although the coefficient is not significant at the 5% level, but that seems in part to be the result of a higher standard deviation. The coefficient is not that much smaller than other (significant) constructs with a similar effect size ($r^2 = .073$). The higher performance suggests that respondents tended towards agreeing that their online behaviour was influenced by peer pressure. This might suggest a role for reducing peer pressure as a way of reducing cyber aggression inclination, assuming that the non-significant result is a quirk of our data. It certainly seems to suggest that the role of social/peer pressure, separate to subjective norms would be a useful avenue for future investigation.

**Implications for Research and Practice**

In the development of the hypotheses, several theories informed the direction of the current research. The findings suggest that we can strengthen some of the theoretical perspectives discussed earlier and provide theoretical contributions to a new understanding of cyber aggression from various perspectives. For example, in developing H1, we used Social Ecology Theory to examine the association between (lack of) empathy and aggression. Based on our finding, we can strengthen the argument that individuals interact with varying social contexts or ecological systems and in doing so, influence and are influenced by social relations and the broader culture (Swearer & Espelage, 2004). Similarly, H2 was developed based on Social Cognitive Theory and The General Aggression Model. Our findings are consistent with these theories. Our findings also support the notions presented in Social Learning Theory used to develop H4, where it was argued that cyberbullying perpetration is a learned social behaviour. Social Learning Theory was originally designed to theorise about crime in the physical world. However, our application of the model to virtual worlds extends the applicability of the model in new social contexts (Lowry et al., 2016).

This research adds strength to the argument that situational factors, particularly the behaviour of peers and other social actors around us influence our online behaviour. Specifically, we find that social pressure, low self-control and perceived anonymity show the strongest associations with CAI. The anonymity afforded by online social spaces does appear to contribute to deviant online behaviours. The lack of support for associations between CAI and prior victimisation, incident severity and social pressure suggest an avenue for future research using both quantitative and qualitative data to get a better understanding of how they relate to CAI.

The study also has practical implications. For example, consider the study of the variables “subjective norms” and “social pressure”. While normative beliefs and social pressure are mostly studied as interchangeable constructs (Dang & Liu, 2020; Leone & Parrott, 2019; Piccoli et al., 2020; Xu et al., 2016), the current study explored them as separate variables. This is a unique contribution that highlights the importance of further research into these separate constructs in online social settings. Current findings also suggest that negative normative beliefs are associated with CAI. This finding can influence the policies adopted by social networking communities against aggressive actions. These community policies can serve as a behavioural norm for members, and thereby contribute to the reduction of aggressive behaviours in SNS (Butterfield et al., 2000; Valentine & Bateman, 2011; Xu et al., 2016).

The current study highlights the importance of subjective norms for cyber aggression inclination; this has implications for Social Networking Site content providers. Specifically, trying to influence positive subjective norms (through content posted) may discourage aggressive online behaviours. Previous research shows that it is possible to manipulate subjective norms so as to change behavioural intentions (Grimes & Marquardson, 2019). Therefore, promoting more positive subjective norms may enable levels of aggression to be mitigated.

As subjective norms are associated with people who are close to or important to individuals who engage in cyber aggressions, social media and government law enforcement bodies can consider this second layer of the responsibility networks and initiate some form of social adjustment and orientation program. Using the Covid-19 pandemic as an analogy, the health and safety measures directed at Covid-19 victims differ from those directed
at the victims' associates. As cybercrimes have long-term impact and can themselves operate as CAI triggers, it is important to establish a legal framework that identifies as two separate but related groups (i) the perpetrators of aggressive acts online, and (ii) the perpetrators' associates, and implements measures that treat each group appropriately. As noted above, the role of social pressure, as distinct from subjective norms, would merit further investigation. Although non-significant in our model, the effect size and path coefficients are of similar magnitude to other (significant) results. This might suggest that there is something else influencing the effect of social pressure on cyber aggression behaviour.

The positive association between the impulsive use of SNS and CAI may indicate that socialisation is key to reducing the level of CAI by enhancing the ability of social media users to practise self-discipline. This might be achieved by nurturing socialisation processes within societies and organisations, highlighting their relevance to religious beliefs and orientations, and emphasising them in the training and education programs, ethics, CSR, and sustainability practices of various private and public sector organisations, and even in the rules and regulations of countries.

Individual perception of online anonymity can be influenced through Social Networking Site design. Developers can introduce measures that prevent social media profiles being created anonymously (Correa et al., 2021; Stutzman & Hartzog, 2012; Gerhart & Kookhikamali, 2019). This may reduce the sense of safety and power felt by aggressors when using SNS for delinquent acts. Also, intervention strategies can be used where appropriate (e.g., automatic identification/filtering of aggressive posts on SNS; Barlett et al., 2020; Kim et al., 2020; Kumari et al., 2019; Modha et al., 2018, 2020). Creating awareness among users about the availability of built-in extensions of the social network to protect against cyberbullying is another consideration (Kintonova et al., 2021). Accordingly, we recommend that social media firms incorporate software features that reduce the disinhibition effect that can be arise from anonymity (such as linking a real name and contact details to a username).

Limitations

Some limitations in the current study should be acknowledged. First, the sample size, although meeting the analytical criteria of PLS-SEM, is small. As our results were obtained from a cross-section study, we can only draw conclusions regarding association. A longitudinal (larger scale) study would help to explore causation between the variables.

The current research found four of the eight hypotheses to be unsupported. This may be due to the small sample size. As the study found no evidence in relation to the social desirability bias of responses. The online survey could be improved with new and revalidated items in a future study involving a larger sample. For example, multidimensional concepts such as perceived anonymity can be studied in detail as social anonymity, visual anonymity, definitive anonymity, location anonymity, and technical and social anonymity (Choi et al., 2016; Hayne & Rice, 1997). Further, we did not directly ask participants to report whether they had religious beliefs. Therefore, it is not possible to disentangle participants responses to the religiosity scale according to whether participants held religious beliefs and disagreed with the scale items or whether they did not have religious beliefs. As the nature of the impact of contributing factors might be moderated or mediated by the demographics of the respondents, future study design might consider possible moderators and mediators. For example, the association between religiosity and criminal offending could be considered, given the argument that it may be mediated by self-control (Reisig et al., 2012).

A further limitation is that the current study relied on self-report methods and adopted a cross-sectional design. Therefore, it was not possible to fully explore whether intent translates into behavioural experiences or the extent to which the behaviour is cyclical in nature. Therefore, researchers may want to consider implementing longitudinal designs to allow a further exploration of the direction of the reported relationships and experiential methods as a mechanism to overcome memory bias (Scollon et al., 2003).

Conclusions

This study aimed to explore the concept of cyber aggression inclination and the personal and situational factors that contribute to it. The extant literature suggests that there is a paucity of empirical research exploring the concept of “cyber aggression”, particularly in the context of SNS (e.g., Suzor et al., 2019; Zhong et al., 2020; Zhu et al., 2020). Drawing inferences from various theories, we developed a theoretical framework using eight
hypotheses that explore the links between personal and situational factors and CAI. Partial Least Squares-Structural Equation Modelling (PLS-SEM) was used to assess measurement, structural models, and hypotheses testing.

The findings suggest that three personal factors (virtual empathy, self-control, subjective norms) and one situational factors (intrinsic religiosity) are associated with CAI of SNS users, thereby contributing to the development of a conceptual model on cyber aggression inclination. Interestingly, the findings of the study do not provide statistically significant evidence for the influence of prior aggression victimisation, social pressure, and perceived incident severity on CAI. Overall, the study contributes to the advancement of various theories such as the General Aggression Model, Social Identity Theory, Theory of Planned Behaviour, the social identity model of deindividuation effects, Social Ecology Theory, and the General Theory of Crime and provides several important practical implications for key stakeholders in the social media industry. For example, our findings are relevant to the policies being adopted by social networking communities seeking to counter or reduce aggressive actions. The study also emphasises the role played by socialisation processes in reducing cyber aggression behaviour by social media users. We make the case for a wholesale adoption of these socialisation processes at organisation-, country- and global-level.

Footnotes

1 Respondents were asked to rate the following incidents on a scale of 1 (Not a severe incident) to 5 (A very severe incident):

1. Damaging someone else's reputation by spreading rumours about them on SNS.
2. Liking and commenting on posts on SNS that are intended to bully a person/group (e.g., religious group)
3. Resharing a post containing hateful comments about a certain person/group (e.g., religious group) on SNS.
4. Insulting another person/group (e.g., religious group) publicly on SNS.
5. Posting embarrassing photos or videos of someone else on SNS.
6. deliberately excluding someone from an online social group to make him/her feel excluded.
7. Sending threatening messages/reactions to someone on SNS.

Conflict of Interest

The authors have no conflicts of interest to declare.

Authors’ Contribution

Hemamali Tennakoon: conceptualization, investigation, data curation, methodology, formal analysis, writing—original draft, writing—review & editing. Lucy Betts: conceptualization, investigation, writing—original draft, writing—review & editing. George Saridakis: methodology, formal analysis, writing—original draft, writing—review & editing. Chris Hand: methodology, formal analysis, writing—original draft, writing—review & editing. Anil Chandrakumara: conceptualization, writing—original draft, writing—review & editing.

References


About Authors

Hemamali Tennakoon is a Senior Lecturer in Strategy and Management at Brunel Business School (BBS), Brunel University London. She received her PhD in Online Information Security, Privacy and Social Commerce from Kingston University, London. Her research has appeared in peer-reviewed journals including Computers in Human Behaviour, Information Technology & People, and International Journal of Human-Computer Studies. Hemamali is a Fellow of the British Computer Society. Her main research interests include cyberpsychology, digital anthropology, online privacy and security.

https://orcid.org/0000-0003-1526-0254

Lucy Betts is Professor of Social Developmental Psychology at Nottingham Trent University. Her research interests are in social developmental psychology, focusing on cyberbullying experiences, perceptions of online risk and understand the distinction between bullying and banter.

George Saridakis is a Professor of Small Business and Entrepreneurship and the Head of the Department of Marketing, Entrepreneurship, and International Business (MEiB) at Kent University. He holds a Ph.D. in Economics from Essex University. His research has been presented at numerous conferences, and he is the recipient of many distinctions, honours, and prizes. He has published several journal articles, edited books, book chapters, and official reports. Additionally, he holds an honorary position at The University of the West Indies.

Chris Hand is Professor of Marketing at Kingston Business School. His research focuses on consumer behaviour and applications of quantitative methods to management issues. His research has appeared in journals including the Journal of Business Research, Information Technology & People, Behaviour & Information Technology and Economic and Industrial Democracy.

Anil Chandrakumara earned his PhD in International Organisational Behaviour (OB) and Management from the University of Sheffield (UK). His research work is published in several international journals such as the International Journal of Manpower, Employee Relations International Journal, Thunderbird International Business Review, Australian Accounting Review, International Journal of Management, Corporate Ownership and Control, International Employment Relation Review, and in proceedings of international conferences. His current teaching-research nexus includes international OB, Cross-cultural management, Global business strategy, Ethics, CSR, and Sustainability in institutional and global context.

Correspondence to
Hemamali Tennakoon, Brunel Business School, Kingston Lane, Uxbridge, UB8 3PH, United Kingdom, hemamali.tennakoon@brunel.ac.uk