Received: 25 June 2021 | Accepted: 5 January 2022

DOI: 10.1111/hojo.12485

The Howard Journal of Crime and Justice | Howard League for Penal Reform

WILEY

ORIGINAL ARTICLE

Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types

Suleman Lazarus[1] | **Mark Button**[2] | **Richard Kapend**[3]

[1]Suleman Lazarus is a Visiting Fellow, the Mannheim Centre for Criminology, London School of Economics and Political Science (LSE)

[2]Mark Button is the Founder and Director, Centre for Counter Fraud Studies, Institute of Criminal Justice Studies, University of Portsmouth

[3]Richard Kapend is a Senior Lecturer in Criminology and Quantitative Research Methods, University of Portsmouth

Correspondence
Suleman Lazarus, Visiting Fellow, the Mannheim Centre for Criminology, London School of Economics and Political Science (LSE).
Email: suleman.lazarus@gmail.com

Abstract

Do men and women perceive cybercrime types differently? This article draws on the distinction between socio-economic and psychosocial cybercrime proposed by Lazarus (2019) to investigate whether men and women hold different perceptions of digital crimes across these two dimensions. Informed by the synergy between feminist theory and the Tripartite Cybercrime Framework (TCF), our survey examined respondents' differential perceptions of socio-economic cybercrime (online fraud) and psychosocial cybercrime (cyberbullying, revenge porn, cyberstalking, online harassment) among men and women in the United Kingdom. The results revealed that women considered psychosocial cybercrime worse than men. Conversely, we found no differences between men and women with regard to socio-economic cybercrime. The article concludes that psychosocial cybercrimes are more gendered than socio-economic cybercrime, suggesting problems with the meaning of 'cyber-enabled crimes', and substantiating the synergy between the TCF and feminist perspectives.

KEYWORDS
cybercrime classifications, cybercrime taxonomy, digital divide, feminist criminology, gender differences, misogyny online, online fraud, perceptions of cybercrime, romance scams, Tripartite Cybercrime Framework (TCF)

1 | INTRODUCTION

This article explores the value of feminist theory in understanding digital crimes. Social and situational constructions of gender offline are concurrently impactful in cyberspace (Jane, 2016, 2018; Mumporeze & Prieler, 2017). Indeed, online attitudes, behaviours and perceptions are extensions of offline social processes and relationships in society (Citron, 2014; De Kimpe et al., 2018; Jane, 2016; Li, Coduto & Morr, 2019; Mumporeze & Prieler, 2017). Empirical evidence from many nations such as Russia (Khlomov, Davydov & Bochaver, 2019), Rwanda (Mumporeze & Prieler, 2017), China (Liong & Cheng, 2017; Min & Shen, 2020), Finland (Koiranen et al., 2019), India (Ahmed, Cho & Jaidka, 2017), Taiwan (Lai, Hsieh & Zhang, 2019), Syria (Öztürk & Ayvaz, 2018), Nigeria (Lazarus & Button, in press; Lazarus & Okolorie, 2019), Australia (Hutchings & Chua, 2017), Malaysia (Shaari et al., 2019), Germany, Switzerland, the United Kingdom and the United States (Eckert, 2018) demonstrate the direct connection between online and offline behaviours and relationships. Before the digitalisation of crimes, women (and girls) were shown to be more fearful of traditional crimes than men (and boys) (Box, Hale & Andrews, 1988). Likewise, in recent years, studies have shown that women are more fearful than men that abuse on the Internet will result in physical harm (Office for National Statistics, 2017a, 2017b). Differences between men and women in the virtual world are connected to long-standing gender issues in society, and therefore gender issues in cyberspace are likely to persist as long as they exist offline (Eckert, 2018; Jane, 2016; Mumporeze & Prieler, 2017).

Consequently, we argue that who is victimised, why, and to what effect applies differently to digital crimes that are more psychologically motivated (e.g., online revenge porn) than those that are more financially motivated (e.g., online fraud) (based on the distinction between socio-economic and psychosocial cybercrime (Lazarus, 2019)). This warrants the examination of the connections between gender and cybercrime types, as a critical starting point. In other words, it is vital to disaggregate cybercrime types to demonstrate their differential, gendered impacts. Accordingly, this study asks: Do men and women perceive cybercrime types differently? This article aims to: (i) investigate perceptions of the different forms of digital crimes across gender; and (ii) advocate for the centrality of gender as a theoretical starting point for the investigating of various types of digital crimes. We present the rest of the study as follows: theoretical background (section 2), methods (section 3), findings (section 4), discussion (section 5) and conclusion (section 6).

2 | THEORETICAL BACKGROUND

2.1 | Feminist criminology perspectives

Feminist criminology advocates a more critical examination of gender issues in society to understand crime (Burgess-Proctor, 2006; Carrington, 2014, 2017; Chesney-Lind, 2020; Sabon, 2018). Feminist criminology perspectives are not simply the study of crimes committed by

women (and girls), nor are they just studying women/girls as victims of crime (Carrington, 2014; Chesney-Lind, 2020; Lynch, 2018; Naegler & Salman, 2016). For example, while many gender differences appear in statistical investigations about crime, most of them are rarely expressed and embedded in the feminist epistemology of crime (Chesney-Lind, 2020; Gustafson, 1998; Smith & Torstensson, 1997). The feminist epistemology of crime explicitly takes into account: (i) the unequal power relation between boys/men and girls/women; and (ii) the differences between boys/men's and girls/women's perceptions and experiences of the world, in its approach to the study of crime and gender (Chesney-Lind, 2020; Lynch, 2018; Sabon, 2018; Sharp, 2015). Many scholars have demonstrated that gender is situationally accomplished, socially constructed, and culturally performative, and its persistence as a significant factor in people's lives is remarkable (Chesney-Lind, 2020; Connell & Messerschmidt, 2005; Cook, 2016; hooks, 2000; Ibrahim, 2015; Lazarus et al., 2017; Oakley, 2018; Stambolis-Ruhstorfer & Tricou, 2017). Accordingly, this article acknowledges that gender intersects with multiple axes of social (dis)advantages such as age. Thus, feminist perspectives encompass the use of an intersectional theoretical framework to examine how conceptions of gender and crime interact (Burgess-Proctor, 2006; Carrington, 2014). Feminist criminologists examine these interactions in offline contexts, but it is important to identify how these extend to the virtual (Lazarus, 2019). Therefore, it is a valuable lens/approach exploring the risk/crime perception research (e.g., Gustafson, 1998; Painter, 1992), where prior works have consistently established gender differences. Accordingly, we now focus on gender differences in risk/crime perceptions.

2.2 | Gender differences in risk/crime perceptions

In perceptions of risk or crime, gender makes a difference. Many scholars such as Gustafson (1998), Smith & Torstensson (1997), Davis & Dossetor (2010) and Choi & Merlo (2021) have consistently established that gender differences matter as far as perceptions of crime are concerned. These authors demonstrated many years ago that gender differences in the perception of risk/crime reflect the gendered ideology and gendered practice alongside gender structures (e.g., Choi & Merlo, 2021; Gustafson, 1998; Smith & Torstensson, 1997). Gender socialisation, for example, is an essential aspect of gender differences in crime perception. First, women (and girls) are generally socialised to place relatively low value on fighting, taking punches, and other physical abilities, unlike men (and boys). At the same time, men and boys are socialised to deny fear more than are women and girls (Smith & Torstensson, 1997). Second, the media, parents, the police and public authorities generally produce and tailor warnings of danger and precautionary advice for women (and girls) more than for men and (boys) (Gustafson, 1998; Smith & Torstensson, 1997). Such socialisation patterns concerning fear and physical vulnerability may influence women's dependency on the men in their lives for security and protection offline. In turn, it also shapes the gender differences in perceptions of crimes and risks. Other forces in society, such as unequal power relations between men and women, also create multiple dimensions and positions regarding gender differences (Burgess-Proctor, 2006; Chesney-Lind, 2020; Gustafson, 1998; Painter, 1992).

Indeed, the social control of women by men, men's dominance over women, and the vulnerabilities of women, produced and maintained in relational processes, are implicated in perceptions of risks and crimes (according to feminist research about traditional crimes) (Connell & Messerschmidt, 2005; Cook, 2016; hooks, 2000; Gustafson, 1998; Painter, 1992). Comparably, 'victims of traditional crimes largely have the same needs as victims of digital crimes' (Leukfeldt, Notté & Malsch, 2020, p.73). Research on crimes on the Internet illuminates the idea that sexually

motivated crimes (e.g., rape threats and sexual harassment online) are perceived as more frightening for women (and girls) than for men (and boys) (e.g., Eckert, 2018; Walker & Sleath, 2017). It may well be that those most victimised by psychological crimes on the Internet (e.g., women and girls) are those most fearful of these crimes. There is certainly no doubt that gender identity is a critical factor in accounting for the gap in fear of crime between men and women (Choi & Merlo, 2021; Gustafson, 1998; Smith & Torstensson, 1997). This reinforces the fact that people socialised as feminine in society are less likely to suppress their expression of fear than those socialised as masculine. Thus, the gender disparities in crimes on the Internet merit attention, not the least, because they are crucial in critiquing the term 'cybercrime' particularly the cyber-enabled and people-centric classifications.

2.3 | The meaning of cybercrime and ambiguities

Cybercrime refers to any criminal activity carried out through the use of Information Communication Technology (ICT) and the Internet (Button & Cross, 2017; Hall et al., 2021; Iacobucci et al., 2021; Jaishankar, 2018; Leukfeldt, Notté & Malsch, 2020; Park et al., 2019). It has been defined in different jurisdictions and by many scholars (Adogame, 2009; Button et al., 2014; Hall et al., 2021; Jaishankar, 2018; Lazarus, 2020a, 2020b; Park et al., 2019; Powell, Stratton & Cameron, 2018; Yar & Steinmetz, 2019) and security agencies (e.g., Interpol, 2020; Kaspersky, 2020) to mean slightly different things. However, the most consistent idea is that the term 'cybercrime' is an umbrella word for a wide spectrum of digital crimes such as cyber espionage, cyberstalking, online fraud, cyberbullying, online revenge pornography, and the distribution of computer viruses (Gordon & Ford, 2006; Lazarus, 2019; Yar & Steinmetz, 2019). The term 'cybercrime' on the one hand, is overly broad, and on the other, it is rigid, and by implication, it is resistant to change because it is 'loosely' used in everyday parlance as a simple 'acronym' for all forms of crimes on the Internet (Lazarus, 2019, p.18).

Consequently, there is a fairly clear pattern to suggest that in using the term 'cybercrime' as a given, multitudes of researchers 'clump together' a wide spectrum of digital crimes with arbitrary attributes (e.g., Bidgoli & Grossklags, 2017; Sabillon et al., 2017). The homogenisation of crimes with different core attributes inhibits a more critical examination of gender nuances in a wide spectrum of digital crimes. To illustrate, all five digital crimes in this study listed in Table 1 are cyber-enabled or people-centric cybercrimes.

However, the 'cyber-enabled crimes' (McGuire & Dowling, 2013) or 'people-centric cybercrimes' (Gordon & Ford, 2006) classification encompasses a broad spectrum of digital crimes with arbitrary attributes. As a result, they are ill-equipped to differentiate between digital crimes, such as 'fraudulent sales online' and 'cyberbullying' illustrated in Figure 1, adapted from Ibrahim (2016, p.46).

To illustrate further, online revenge porn and online fraud (e.g., fraudulent sales on eBay) involve different motivations, victim-perpetrator gains/losses and victim-perpetrator relationship/dynamics, as shown in Table 2. Consequently, these terms (e.g., people-centric cybercrimes) obscure the meaning of each cybercrime type they represent (for a comprehensive critique of cybercrime and cyber-enabled or people-centric categories, see Ibrahim (2016); Lazarus (2019)).

This article sets out to highlight the analytic consequences of this homogenisation. It does so by highlighting the significance of distinguishing different types of cybercrime for understanding the gendered nature of many forms of crime, drawing on the Tripartite Cybercrime Framework (TCF).

TABLE 1 Operational definitions of the five cybercrime types

Cybercrime types	Categories	Operational definitions
Cyberbullying	Psychosocial	Bullying is intentional, aggressive behaviour, carried out repeatedly against a victim, whereas with cyberbullying, the power imbalance between bully and victim and the repetitiveness of the behaviour typically involved in traditional bullying are often missing from the equation.
Online harassment	Psychosocial	Online harassment can be defined as the act of aggressively pressuring, intimidating, distressing or spreading denigrating rumours about others.
Online fraud	Socio-economic	Online fraud refers to the computer and/or Internet-mediated acquisition of financial benefits by false pretence, impersonation, manipulation, counterfeiting, forgery or any other fraudulent representation of facts.
Revenge porn	Psychosocial	Revenge porn is defined as non-consensual sharing of sexually explicit images and/or videos, whether self- or other-generated, with an underlying motivation linked to revenge.
Cyberstalking	Psychosocial	Cyberstalking or cyber dating abuse refers to using the Internet and other technological devices to monitor or harass another person in a threatening way.

Source: modified from Lazarus (2019, p.22).

TABLE 2 Perpetrators' benefit and victims' losses

Attacker/Attacked	Socio-economic	Psychosocial	Geopolitical
Perpetrator (primary benefit)	Economic gain	Psychological gain	Geopolitical, economic & psychological gain
Victim (primary loss)	Economic loss	Psychological loss	Geopolitical, economic & psychological loss
Perpetrator (secondary benefit)	Psychological gain	Economic gain	Geopolitical, economic & psychological gain
Victim (secondary loss)	Psychological loss	Economic loss	Geopolitical, economic & psychological loss

Source: from Ibrahim (2016, p.47).

2.4 | The Tripartite Cybercrime Framework (TCF)

A nascent typology suited to investigating the linkages between gender and digital crimes is the TCF proposed by Ibrahim (2016) and developed further by Lazarus (2019). According to the TCF, cybercrime can be divided into three broad motivational parts: socio-economic; psychosocial; and geopolitical.

- **Socio-economic** cybercrime can be defined as the computer or/and Internet-mediated acquisition of financial benefits by false pretence, impersonation, manipulation, counterfeiting,

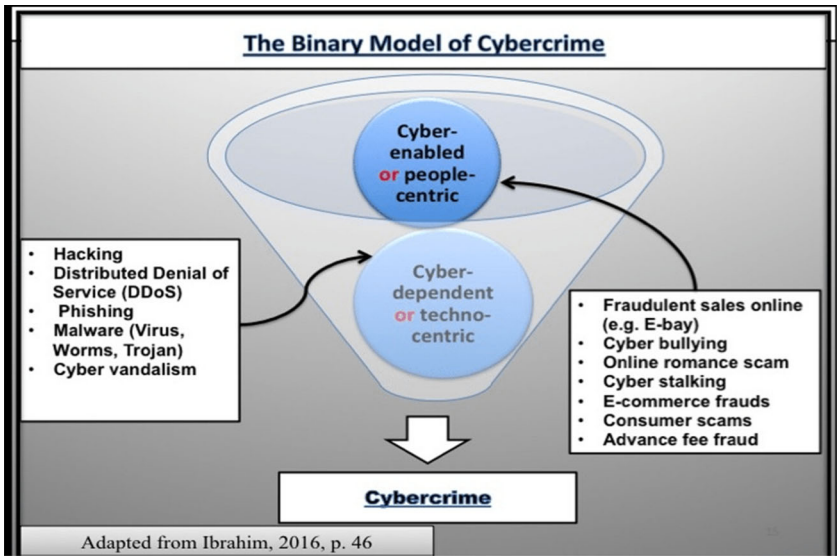

FIGURE 1 The cybercrime dichotomy

forgery, or any other fraudulent representation of facts such as online fraud, credit card fraud, online embezzlement and romance scams.

- **Psychosocial** cybercrime refers to digital crimes that are primarily psychologically driven to cause shock, distress or harm to a person, where monetary gain is not the primary objective. They include cyberstalking, cyberbullying, and online harassment.
- **Geopolitical** cybercrimes include cybercrimes that are fundamentally political in nature and involve agents of the state (and non-state activists) and/or their representatives engaged in acts such as cyber espionage or malware-based attacks to disrupt the critical national infrastructure of a state.

These categories are, of course, not always mutually exclusive; for example, hacktivists exposing stolen personal data from police officers as a political protest could have psychosocial and geopolitical consequences simultaneously. Nevertheless, the TCF provides a valuable heuristic for distinguishing key properties of different cybercrimes, and acknowledges the importance of different motivations, gains, and losses associated with these three groups (i.e., socio-economic, psychosocial, and geopolitical groups outlined in Table 2). Hence, because structured gender relations retain their efficacy in online contexts, this research will particularly benefit from the TCF.

2.5 | The overlap between feminist perspectives and the TCF

The TCF facilitates a feminist analysis of cybercrime. The characteristics of the TCF outlined in Table 2 themselves align the TCF with the feminist epistemology of crime in the discussion of digital crimes. Both the TCF and feminist perspectives locate gender at the core of crime investigation and acknowledge that contextual cultures and nuances apply online as they do offline. Feminist epistemology of crime locates gender at the core of crime investigation and acknowledges the

sources of social advantage and disadvantage in society (Chesney-Lind, 2020; Cook, 2016). While sources of social advantage and disadvantage are related to patterns of offending and victimisation, gender is one of the critical sources of social advantage and disadvantage in society (Lazarus, 2019). The TCF recognises that perpetrators and victims of a wide spectrum of digital crimes have a unique relationship and that this relationship is fundamentally based on the perpetrators' primary motivations and benefits and the victims' primary losses, as shown in Table 1. For example, online abuse disproportionately affects women and online abuse of women is not fully recognised as entangling online and offline communication (Eckert, 2018). Conceptually, the TCF, therefore, offers a framework that is able to situate gender at the core of the analysis of cybercrimes. In this empirical illustration of these properties of the framework, we focus on just socio-economic and psychosocial cybercrimes.

2.6 | Contrasting the socio-economic and psychosocial cybercrimes types

We focus on the socio-economic and psychosocial cybercrime types in recognition of the fact that the motivations, victimisations, and relational processes involved in these two parts of the TCF are more connected with the broader online experiences of individuals than the geopolitical category. There are relevant distinctions between the groups in terms of their consequences, as illustrated in Table 2. For example, there is a reasonably clear pattern that victims of psychosocial cybercrimes such as revenge porn and cyberbullying directly and primarily experience a range of similar emotional, psychological, and behavioural health consequences, according to multiple comprehensive review articles on four psychosocial cybercrime types included in this present study: (see (i) Walker & Sleath's (2017) review of 82 published works on revenge porn; (ii) Watts et al.'s (2017) review of 54 published articles on cyberbullying; and (iii) Stevens, Nurse & Arief's (2021) review of 43 articles on cyberstalking and online harassment for fuller analyses). These consequences include anxiety, self-harming, depression, low self-esteem, and suicidal ideation to varying degrees (Stevens, Nurse & Arief, 2021; Walker & Sleath, 2017; Watts et al., 2017). However, in addition to the direct psychological costs of psychosocial cybercrimes, coping with these psychologically based crimes can have indirect financial consequences. For example, costs associated with therapy, residential mobility, and time taken off work can negatively impact victims of psychosocial cybercrimes financially. The same primary and secondary losses are not found for socio-economic cybercrime types such as online fraud, even though there may be psychological consequences of being victims of fraud.

Some researchers (Hai-Jew, 2020; Kopp et al., 2016; Shaari et al., 2019; Whitty & Buchanan, 2012) also suggest that the act of deception involved in online fraud can be driven by a non-monetary reward such as a psychological thrill. Equally, they argue that a financial loss due to online fraud can manifest in the victim physiologically as distress. However, the above researchers (e.g., Hai-Jew, 2020; Kopp et al., 2016; Whitty & Buchanan, 2012) primarily focused on romance scams. Therefore, we spotlight here that in romance scams, scammers like lovers, invoke strong emotions in the romantic relationships and use the development of love affairs as a toolbox to lure their victims into offering money to them.[1] Also, for scammers, it does not matter if the owner of the money is a man or woman; scammers consider victims to be 'good clients' inasmuch as they can steal funds from them without much ado (e.g., Lazarus, 2018). Accordingly, we define romance scams as the deployment of fake romantic relationships primarily for material ends. Thus, the finding above (e.g., Hai-Jew,

2020; Kopp et al., 2016; Shaari et al., 2019; Whitty & Buchanan, 2012) regarding the negative psychological consequences for victims may be particularly marked – given that romance scams are in the realm of love and friendship. Such consequences may not be incurred for victims of other forms of online fraud (e.g., insurance fraud). Arguably, the intimacy between the victim and perpetrator of romance scams is chiefly accountable for the strong manifestation of psychological distress in victims, since romance scams are embedded in love affairs.

As Button & Cross (2017), Button & Whittaker (2021), Goutam & Verma (2015) and Button, Hock & Shepherd (2022) have noted, online fraud includes a wide range of acts, such as non-delivery fraud, credit card scam, identity theft, intellectual property crimes, and romance scams. All are conducted with the primary aim of securing a financial benefit for the perpetrator. Thus, online fraud is rooted essentially blind in relation to gender (Lazarus, 2019). For example, online banking customers' victimisations discussed in Jansen & Leukfeldt's (2016) study were not targeted on the basis of their gender. But the same cannot be said regarding psychosocial cybercrimes such as revenge porn and cyberbullying, which are fundamentally more expressive or relational than socio-economic cybercrimes, and overwhelmingly are conducted by men targeting women. The negative experiences of adolescent girls in terms of cyberbullying, and online harassment, which have been highlighted in Burgess-Proctor, Patchin & Hinduja (2009), have no economic motivations at their heart. Similarly, the negative experiences of women bloggers in terms of cyberstalking, cyberbullying, and rape threats (Eckert, 2018) cannot be attributed to economic motivations. These women bloggers in Germany, Switzerland, the United Kingdom and the United States were victimised on the basis of their gender (Eckert, 2018). The bloggers' negative experiences (Eckert, 2018) and that of adolescent girls (Burgess-Proctor, Patchin & Hinduja, 2009) reflect contemporary social organisation and men's domination over women.[2]

Cultural forces socialise men and women as masculine and feminine individuals (Connell & Messerschmidt, 2005; hooks, 2000; Oakley, 2018). As a consequence, men and women perceive and experience the virtual world distinctively (Eckert, 2018; Marganski, 2020; Sherman et al., 2000; Stavropoulos et al., 2021; Steinmetz, Holt & Holt, 2020; Vella et al., 2020). Such differences are apparent in the relational processes that characterise psychosocial cybercrime types, such as online abuse and harassment (Lazarus, 2019). While such crimes are experienced as psychologically damaging by women, they are often downplayed or dismissed by men. For example, Steinmetz, Holt & Holt (2020) describe respondents recounting how: 'if [a woman] complains about being harassed or bothered, the general reaction is "what did you expect? You're a girl, and they never defend you or ask the annoying guys to shut the fuck up. And if you tell them to shut the fuck up, then that leads them to attack you more"' (p.942). Thus, it is reasonable to suggest that psychosocial cybercrimes such as cyberbullying and online harassment manifest more through relational processes than socio-economic cybercrimes such as online fraud. By the same token, who is victimised, why, and to what effect, apply more to psychosocial cybercrime types (e.g., online harassment, cyberbullying, revenge porn, and cyberstalking) than the socio-economic category (e.g., online fraud) (Lazarus, 2019).

The contrast between the socio-economic and psychosocial cybercrime types resonates with the discrepancies between men's and women's views and experiences of crimes on the Internet (Lazarus, 2019), which is reflective of the broader questions of gender in society. Thus, while the study of gender issues inevitably involves comparisons, such comparisons are essential to advancing our understanding of the psychology of gender more broadly and how women and men may perceive some crimes on the Internet distinctively (Eagly, 2016). For example, many qualitative studies (e.g., Adeduntan, 2022; Cassiman, 2019; Ibrahim, 2017; Jansen & Leukfeldt, 2016; Lazarus, 2018; Lazarus & Button, in press; Lewis, 2020), quantitative studies (e.g., Barnor et al., 2020;

Wang, Nnaji & Jung, 2020), and review articles (e.g., Hall et al., 2021; Lazarus, 2020b) on socio-economic cybercrime category suggest that victims are not targeted based on their gender.

On the flip side, comprehensive reviews of published studies on psychosocial cybercrime types tell a different story. For example, Walker & Sleath's (2017) review of 82 published works on revenge porn, Watts et al.'s (2017) review of 54 published articles on cyberbullying, and Stevens, Nurse & Arief's (2021) review of 43 articles on cyberstalking and online harassment suggest that victims of this psychosocial cybercrime category were primarily targeted on the basis of their gender. This article aims to illustrate that psychosocial cybercrimes are more gendered than socio-economic cybercrimes. Since victims of this psychosocial cybercrime category were primarily targeted as women/girls, unlike victims of socio-economic cybercrime, we, therefore, hypothesise that perceptions of different types of cybercrime will also differ in line with this differential targeting. Specifically, we hypothesise that:

(i) There is no gender effect on the perception of how severe the socio-economic cybercrime types are.
(ii) There is a gender effect on the perception of how severe the psychosocial cybercrime types are.

2.7 | How this present work differs from previous contributions

This present article differs from previous contributions in multiple ways. First, while the TCF has served as a reference point for some studies (De Kimpe et al., 2020, p.18; Iacobucci et al., 2021, pp.195–196; Park et al., 2019, p.5; Solano & Peinado, 2017, p.1), no study has empirically examined whether perceptions of cybercrimes differ in line with the distinctions in the TCF. The article is also the first empirical study to demonstrate the synergy between the TCF and feminist epistemology of crime.

3 | METHODS

3.1 | Participants

The full sample comprised 407 respondents (men: 38.1%, n = 155; women: 60.9%, n = 248, four participants did not give their gender, we, therefore, focus on the 403 who did). This sample size is consistent with prior survey studies on Internet behaviour, such as Liong & Cheng's (2017) study based on 381 Chinese students and Stavropoulos et al.'s (2021) study based on 404 World of Warcraft gamers (see also Lo, Lie & Li, 2016). We used ad hoc recruitment methods. These 407 participants, staff and students, were recruited in total. While we recruited some participants via email from three universities in the United Kingdom, other participants were recruited via Facebook invitation (i.e., Facebook groups associated with these three universities). Accordingly, ethical approval was obtained from a university in the United Kingdom.

We first illustrate the overall composition of the sample before going on to investigate whether the findings on perceptions of cybercrime are in line with our hypothesis. The distribution shows a skewed distribution in favour of women for all six categories. This is simply because there were/are a more significant number of women than men in this study as participants, as shown in Figure 2. A Pearson Chi-squared test was conducted to assess whether gender has an effect

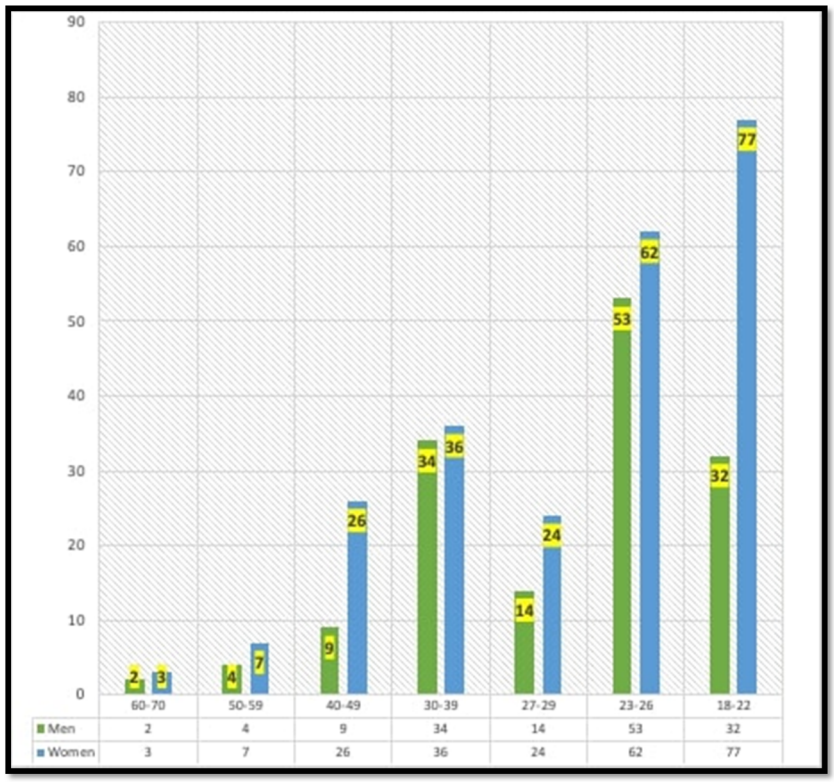

FIGURE 2 Age distribution of respondents

on computer skill and level of proficiency. Results show no statistically significant association between gender and computer skill and level of proficiency; with $p = 0.209$, which is well above the 95% threshold. Any association that may be seen from this distribution would likely have happened by chance.

3.2 | Measures

Participants were informed that participation in the study was voluntary and that data were anonymous and confidential. Participants were asked to complete an online survey, distributed through Google forms which asked principally about their perceptions of different forms of cybercrime. The authors did not assume that participants had the same working definitions. Thus, the authors provided information on how cybercrime types (online fraud, cyberbullying, revenge porn, cyberstalking, online harassment) were defined to participants, which was similar to the information in Table 1. Participants were asked to rate how severely they felt each cybercrime form was on a Likert scale from 1 (not at all severe) to 10 (extremely severe). For example, participants were asked: How would you rate the wrongfulness and seriousness of the following (with 1 being not wrong/serious and 10 being extremely wrong/serious)?

1. Cyber fraud or online fraud
2. Cyberbullying
3. Revenge porn
4. Cyberstalking
5. Online harassment

4 | RESULTS

Women reported all types of cybercrime (i.e., psychosocial cybercrime) as being worse than did men, except for online fraud (i.e., socio-economic cybercrime), where there was no difference between men and women. Specifically, as shown in Table 3, women considered cyberbullying, revenge porn, cyberstalking, and online harassment (i.e., psychosocial cybercrime types) worse than men. This mismatch between men and women was statistically significant for cyberstalking *** and revenge porn and cyberbullying. It is noteworthy that the responses are not representative of the population as a whole, and inferences to the general population cannot be made from these findings. The aim is to test whether women and men responded differently to the questions. Women typically respond more readily to surveys, so the over-representation of women in our sample does not in itself suggest differential selection on relevant characteristics (e.g., attitudes to cybercrime) of men and women.

5 | DISCUSSION

5.1 | Core findings and implications

The study has empirically explored the synergy between the TCF and feminist criminology. Accordingly, our central finding revealed that socio-economic cybercrimes are less gendered than the psychosocial cybercrime types. This core finding supports our hypotheses: (i) There is no gender effect on the perception of how severe the socio-economic cybercrime types are. (ii) There is a gender effect on the perception of how severe the psychosocial cybercrime types are. Consistent

TABLE 3 Perception of the seriousness of five cybercrime types by gender – independent samples t-test

Variables	Mean Score		Statistical significance with p value	
	Men n = 153	Women n = 246		
Cyber fraud or online fraud	8.79	8.75	p = 0.816	ns
Cyberbullying	8.49	8.98	p = 0.007	**
Revenge porn	8.41	9.41	p = 0.001	**
Cyberstalking	7.80	8.60	p = 0.000	***
Online harassment	8.28	8.73	p = 0.019	*

Note: *** $p < 0.001$: difference in mean score is statistically highly significant at the 0.001 level; ** $p < 0.01$: difference in mean score is statistically significant at the 0.01 level; * $p < 0.05$: difference in mean score is statistically significant at the 0.05 level; ns: the observed difference is not statistically significant since $p > 0.05$; where p is statistically significant, it can be submitted that women reported on average a severe perception of the specific type of cybercrime when compared with men; however, the non-probability nature of our sample means that any inferences of statistical significance should be treated with caution.

with our expectations, women reported higher severity for all types of psychosocial cybercrime except for online fraud. This finding can be understood in the context of prior research, which has suggested that women generally perceive crime to be more severe than do men and particularly those crimes that affect them disproportionately, such as online abuse and harassment, resulting in physical harm (Office for National Statistics, 2017a, 2017b; Smith & Torstensson, 1997; Stylianou, 2003). While those most victimised by psychological crimes (women and girls) are those most fearful of these crimes, other factors may also exacerbate the gender gap in perceptions of psychosocial cybercrime types. For example, society generally socialises women/girls generally as feminine and primary recipients of warnings of danger and precautionary advice; consequently, women are less likely to suppress their fear of crime they see as frightening (e.g., revenge porn) than are men (Gustafson, 1998; Smith & Torstensson, 1997). Based on the above remarks, we argue here that gender identity is critical in accounting for the gap in fear of psychosocial cybercrime types between men and women.

Focusing on cybercrimes, this article has enhanced prior research by demonstrating that particular forms of cybercrime – those identified in the TCF as psychological – are regarded as more serious by women. By contrast, women rate economic forms of cybercrime comparably to men in terms of severity. Additionally, it is notable that for men, such economic forms of cybercrime are considered the most serious, whereas, for women, revenge porn is rated as more serious than all other forms of cybercrime. Thus, the article has highlighted the significance of distinguishing different types of digital crimes for understanding the gendered nature of various forms of crime, drawing on the TCF.

This empirical contribution suggests that generalising about 'cybercrime' or distinguishing 'cyber-enabled and people-centric cybercrimes' are inadequate for addressing the gendered impacts of different forms of cybercrime. For example, they have been implicated in obscuring the centrality of gender as a theoretical starting point for examining a multitude of digital crimes in academia (Lazarus, 2019). Such theoretical and terminological oversights in research, in turn, have real-life repercussions. A likely consequence of these omissions in research may mean that many corporations and government agencies may not fully recognise the importance of the gender dimensions of psychosocial cybercrimes in their responses to many forms of these digital crimes (e.g., cyberbullying, revenge-porn, cyberstalking, online harassment). The above theoretical and terminological oversights highlight the originality of this contribution.

5.2 | Originality and implications

This present study is original in multiple ways. First, while the TCF has served as a reference point for some studies (e.g., De Kimpe et al., 2020), no study has empirically examined the contrast between the TCF parts or explored 'the synergy between feminist criminology and the Tripartite Cybercrime' (Lazarus, 2019, p.18) for that matter. Second, this article, like others before it (e.g., Eckert, 2018; Jane, 2018; Marganski, 2020; Vella et al., 2020), has attempted to stimulate more alert and sensitive scholarly approaches to gender issues online. However, unlike these previous studies, the present study is the first empirical treatment of the synergy between the TCF and feminist criminology. Indeed, it has tried to encourage existing scholars not only to situate the TCF at the core of feminist perspectives enquiries but also to stimulate the future generation of scholars to be more sensitive to gender issues online. It has attempted to do so because, for example, generations after generations of scholars, who were unaware of feminist criminology as students, encourage their own students to endorse mainstream theories at the expense of feminist approaches

(Cook, 2016; Eagly, 2016; hooks, 2000). Such an imbalance of power relationship has enormous consequences.

A likely consequence of this mismatch is that 'only the marginal voices whose endeavours fit squarely with the aims and scopes of marginal publication venues (often with low or average impact factors) tend to challenge the orthodoxy of mainstream criminology' (Lazarus, 2019, p.28). As a result, social scientists who endorse feminist perspectives continue to play 'catch up' with those who advocate mainstream criminology approaches concerning the use of data on digital crimes in research just as their predecessors have hitherto been doing in terms of traditional crimes. The problem is deep. A likely consequence of this divide is that many researchers may be inclined to cite or recycle scholarly endeavours that fit within mainstream epistemological tradition at the expense of marginal voices in their efforts to publish in high impact journals.

Thus, we argue that such feminist scholarship is by and large neglected in criminological analysis and in the analysis of cybercrime specifically – we need to do more to move the feminist agenda to the centre in this digital age. Increasing proficiency in ICT and the greater immersion of women in cyber-environments by women cannot be expected to reshape patterns of cybercrimes. They, indeed, may lead to greater exposure to them, especially psychosocial cybercrimes. Equally, as long as the meaning of cybercrime, cyber-enabled crimes and people-centric cybercrimes, are taken as a given in research, windows of opportunities necessary to advance our understanding of gender of many digital crimes discussed in this study will continue to be limited. Additionally, this article has not only evinced that men and women perceive cybercrime types differently, but it has also illustrated the benefits of the synergy between feminist criminology and the TCF to answer its research question: Do men and women perceive cybercrime types differently?

5.3 | Theoretical and empirical limitations

While this study has benefitted from the above theoretical lens, the TCF, however, has its limitations. First, since the apparent boundaries between the TCF categories are somewhat blurred, they could be seen as a loose grouping of cybercrime types. For example, cyberbullying could eventually lead to cyber-extortion or hacktivists exposing stolen personal data from police officers, as political protests could simultaneously have psychosocial and geopolitical consequences. Second, this article has explicitly focused on the binary gender: it has excluded a broader spectrum of gender identities such as transgender and bigender. The focus on a diverse range of non-binary gender identities (e.g., transgender) would have offered the opportunity to understand the lived experiences and nuances of such gender identities. Third, though we observe significant differences between men and women in their perceptions of the seriousness of different crimes, we have not captured their exposure, and we cannot draw generalisable inferences from our non-probability sample. Fourth, the dataset (n = 407), which is the empirical basis of this article, may be considered a small sample size. Nevertheless, we believe that this study offers a useful contribution to the literature and has attempted to move gender analysis of digital crimes 'from margin to centre' with illustrations from a survey. This study represents an invitation to researchers to explore the TCF's synergy and the feminist epistemology of crime and test the differences between the socio-economic and psychosocial cybercrime types further. We believe that more will be accomplished more quickly if we situate the feminist perspectives at the core of inquiries concerning digital crimes.

6 | CONCLUSION

This study has sharpened the distinction between the socio-economic and psychosocial cybercrime types by considering how men's and women's perceptions of these types differ. In particular, the study has highlighted significant differences in perceptions of the seriousness of cyberbullying, cyberstalking, online harassment and revenge porn. In contrast, online fraud is regarded as equally serious by men and women. The psychosocial cybercrime types are those to which women are more vulnerable. Hence, their perceptions reflect that women and girls are disproportionately impacted by these crimes (e.g., Burgess-Proctor, Patchin & Hinduja, 2009; Eckert, 2018) alongside recognition of the significance of their impact. Even if men and women are equally victimised, gender differences will still exist. This is because men and boys are socialised to deny fear more than are women and girls. Also, parents and public authorities generally produce and tailor warnings of danger and precautionary advice for women (and girls) more than for men and (boys) (as previously discussed) (e.g., Gustafson, 1998; Smith & Torstensson, 1997). These long-standing patterns of socialisation of women and men in society may be responsible for these gender differences. Nonetheless, the initial findings presented in this article would benefit from being further tested in a larger and representative sample. But meanwhile, they indicate how not only crimes themselves, but perceptions of them, are deeply gendered.

ACKNOWLEDGEMENTS

We thank Professor Lucinda Platt (London School of Economics and Political Science) for her insightful and comprehensive feedback on the initial draft of this article.

ORCID

Suleman Lazarus https://orcid.org/0000-0003-1721-8519
Mark Button https://orcid.org/0000-0002-4169-2619
Richard Kapend https://orcid.org/0000-0002-9273-9042

ENDNOTES

[1] The development of fake love affairs for material ends, often on dating websites or apps, is what scammers themselves called 'freestyling' or 'freestyle tricks' (see Ibrahim, 2016, p.48; Lazarus, 2018, p.64). While victims of freestyling suffer psychological distress and financial loss, as outlined in Table 2, scammers' primary aim is to improve their economic welfare at their victims' expense (Ibrahim, 2016).

[2] It highlights that gender is a critical index factor that accounts for the gap in fear of psychosocial crimes between men and women.

REFERENCES

Adeduntan, A. (2022) Rhyme, reason, rogue. *Journal of Popular Music Studies*, 34(1), 44–67.

Adogame, A. (2009) The 419 code as business unusual: youth and the unfolding of the advance fee fraud online discourse. *Asian Journal of Social Science*, 37(4), 551–573.

Ahmed, S., Cho, J. & Jaidka, K. (2017) Leveling the playing field: the use of Twitter by politicians during the 2014 Indian general election campaign. *Telematics and Informatics*, 34(7), 1377–1386.

Barnor, J.N.B., Boateng, R., Kolog, E.A. & Afful-Dadzie, A. (2020) *Rationalizing online romance fraud: in the eyes of the offender* (AMCIS 2020 Proceedings. 21, University of Ghana). American Conference on Information Systems (AMCIS).

Bidgoli, M. & Grossklags, J. (2017) End user cybercrime reporting: what we know and what we can do to improve it. In: *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*. Vancouver, BC., Canada: Institute of Electrical and Electronics Engineers (IEEE).

Box, S., Hale, C. & Andrews, G. (1988) Explaining fear of crime. *British Journal of Criminology*, 28, 340–356.
Burgess-Proctor, A. (2006) Intersections of race, class, gender, and crime: future directions for feminist criminology. *Feminist Criminology*, 1(1), 27–47.
Burgess-Proctor, A., Patchin, J.W. & Hinduja, S. (2009) Cyberbullying and online harassment: reconceptualizing the victimization of adolescent girls. In: Garcia, V., Clifford, J.E. & Muraskin, R. (Eds.) *Female victims of crime: reality reconsidered*. Upper Saddle River, NJ.: Prentice Hall.
Button, M. & Cross, C. (2017) *Cyber frauds, scams and their victims*. New York: Taylor & Francis.
Button, M. & Whittaker, J. (2021) Exploring the voluntary response to cyber-fraud: from vigilantism to responsibilization. *International Journal of Law, Crime and Justice*, 66, 100482, pp.1–9.
Button, M., Hock, B. & Shepherd, D. (2022) *Economic crime: from conception to response*. London: Routledge.
Button, M., Nicholls, C.M., Kerr, J. & Owen, R. (2014) Online frauds: learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, 47(3), 391–408.
Carrington, K. (2014) *Feminism and global justice*. New York: Routledge.
Carrington, K. (2017) Feminist criminologies. In: Carlen, P. & França, L.A. (Eds.) *Alternative criminologies*. New York: Taylor & Francis.
Cassiman, A. (2019) Spiders on the world wide web: cyber trickery and gender fraud among youth in an Accra Zongo. *Social Anthropology*, 27(3), 486–500.
Chesney-Lind, M. (2020) Feminist criminology in an era of misogyny. *Criminology*, 58(3), 407–422.
Choi, J. & Merlo, A.V. (2021) Gender identification and the fear of crime: do masculinity and femininity matter in reporting fear of crime? *Victims & Offenders*, 16(1), 126–147.
Citron, D.K. (2014) *Hate crimes in cyberspace*. Cambridge, MA.: Harvard University Press.
Connell, R.W. & Messerschmidt, J.W. (2005) Hegemonic masculinity: rethinking the concept. *Gender & Society*, 19(6), 829–859.
Cook, K.J. (2016) Has criminology awakened from its 'androcentric slumber'? *Feminist Criminology*, 11(4), 334–353.
Davis, B. & Dossetor, K. (2010) (Mis) perceptions of crime in Australia. *Trends and Issues in Crime and Criminal Justice [electronic resource]*, (396), 1–6.
De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L. & Hardyns, W. (2020) Help, I need somebody: examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, 108, 106310, pp.1–11.
De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L. & Ponnet, K. (2018) You've got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics*, 35(5), 1277–1287.
Eagly, A.H. (2016) IV. Has the psychology of women stopped playing handmaiden to social values? *Feminism & Psychology*, 26(3), 282–291.
Eckert, S. (2018) Fighting for recognition: online abuse of women bloggers in Germany, Switzerland, the United Kingdom, and the United States. *New Media & Society*, 20(4), 1282–1302.
Gordon, S. & Ford, R. (2006) On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13–20.
Goutam, R.K. & Verma, D.K. (2015) Top five cyber frauds. *International Journal of Computer Applications*, 119(7), 23–25.
Gustafson, P.E. (1998) Gender differences in risk perception: theoretical and methodological perspectives. *Risk Analysis*, 18(6), 805–811.
Hai-Jew, S. (2020) The remote woo: exploring faux transnational interpersonal romance. In: Hai-Jew, S. *Social world sensing via social image analysis from social media*. Manhattan, KA.: New Prairie Press.
Hall, T., Sanders, B., Bah, M., King, O. & Wigley, E. (2021) Economic geographies of the illegal: the multiscalar production of cybercrime. *Trends in Organized Crime*, 24(2), 282–307.
hooks, B. (2000) *Feminist theory: from margin to center*. New York: Pluto Press. (original work published 1984).
Hutchings, A. & Chua, Y. (2017) Gendering cybercrime. In: Holt, T.J. (Ed.) *Cybercrime through an interdisciplinary lens*. New York: Routledge.
Iacobucci, S., De Cicco, R., Michetti, F., Palumbo, R. & Pagliaro, S. (2021) Deepfakes unmasked: the effects of information priming and bullshit receptivity on deepfake recognition and sharing intention. *Cyberpsychology, Behavior, and Social Networking*, 24(3), 194–202.

Ibrahim, S. (2015) A binary model of broken home: parental death-divorce hypothesis of male juvenile delinquency in Nigeria and Ghana. In: Blair, S.L. & Maxwell, S.R. (Eds.) *Violence and crime in the family: patterns, causes, and consequences (contemporary perspectives in family research*, vol. 9). New York: Emerald Group.

Ibrahim, S. (2016) Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, 47, 44–57.

Ibrahim, S. (2017) Causes of socioeconomic cybercrime in Nigeria. In: *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*. Vancouver, BC., Canada: Institute of Electrical and Electronics Engineers (IEEE).

Interpol (2020) *Cybercrime collaboration services*. Available at: https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services [Accessed 23 March 2022].

Jaishankar, K. (2018) Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology*, 12(1), 1–8.

Jane, E.A. (2016) *Misogyny online: a short (and brutish) history*. London: SAGE.

Jane, E.A. (2018) Gendered cyberhate as workplace harassment and economic vandalism. *Feminist Media Studies*, 18(4), 575–591.

Jansen, J. & Leukfeldt, R. (2016) Phishing and malware attacks on online banking customers in the Netherlands: a qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, 10(1), 79–91.

Kaspersky (2020) *Tips on how to protect yourself against cybercrime*. Available at: https://www.kaspersky.co.uk/resource-center/threats/what-is-cybercrime [Accessed 23 March 2022].

Khlomov, K.D., Davydov, D.G. & Bochaver, A.A. (2019) Cyberbullying in the experience of Russian teenagers. *Psychology and Law*, 9(2), 276–295.

Koiranen, I., Koivula, A., Keipi, T. & Saarinen, A. (2019) Shared contexts, shared background, shared values: homophily in Finnish parliament members' social networks on Twitter. *Telematics and Informatics*, 36, 117–131.

Kopp, C., Sillitoe, J., Gondal, I. & Layton, R. (2016) The online romance scam: a complex two-layer scam. *Journal of Psychological and Educational Research*, 24(2), 144–161.

Lai, H.M., Hsieh, P.J. & Zhang, R.C. (2019) Understanding adolescent students' use of facebook and their subjective wellbeing: a gender-based comparison. *Behaviour & Information Technology*, 38(5), 533–548.

Lazarus, S. (2018) Birds of a feather flock together: the Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists. *Criminology, Criminal Justice, Law & Society*, 19(2), 63–80.

Lazarus, S. (2019) Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework. *International Social Science Journal*, 69(231), 15–33.

Lazarus, S. (2020a) 'Establishing the particularities of cybercrime in Nigeria: theoretical and qualitative treatments' (unpublished doctoral dissertation, University of Portsmouth).

Lazarus, S. (2020b) Where Is the money? The intersectionality of the spirit world and the acquisition of wealth. *Religions*, 10(3), 146.

Lazarus, S. & Button, M. (in press) Tweets and reactions: revealing the geographies of cybercrime perpetrators and the north-south divide. *Cyberphsychology, Behavior, and Social Networking*, 1–17. (see http://eprints.lse.ac.uk/115221).

Lazarus, S. & Okolorie, G.U. (2019) The bifurcation of the Nigerian cybercriminals: narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics*, 40, 14–26.

Lazarus, S.I., Rush, M., Dibiana, E.T. & Monks, C.P. (2017) Gendered penalties of divorce on remarriage in Nigeria: a qualitative study. *Journal of Comparative Family Studies*, 48(3), 351–366.

Leukfeldt, E.R., Notté, R.J. & Malsch, M. (2020) Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims & Offenders*, 15(1), 60–77.

Lewis, J.S. (2020) *Scammer's yard: the crime of black repair in Jamaica*. Minneapolis, MN.: University of Minnesota Press.

Li, S., Coduto, K.D. & Morr, L. (2019) Communicating social support online: the roles of emotional disclosures and gender cues in support provision. *Telematics and Informatics*, 39, 92–100.

Liong, M. & Cheng, G.H.L. (2017) Sext and gender: examining gender effects on sexting based on the theory of planned behaviour. *Behaviour & Information Technology*, 36(7), 726–736.

Lo, S.K., Lie, T. & Li, C.L. (2016) The relationship between online game playing motivation and selection of online game characters: the case of Taiwan. *Behaviour & Information Technology*, 35(1), 57–67.

Lynch, M.J. (2018) Acknowledging female victims of green crimes: environmental exposure of women to industrial pollutants. *Feminist Criminology*, 13(4), 404–427.

Marganski, A.J. (2020) Feminist theories in criminology and the application to cybercrimes. In: Holt, T. & Bossler, A. (Eds.) *The Palgrave handbook of international cybercrime and cyberdeviance*. Cham, Switzerland: Palgrave Macmillan.

McGuire, M. & Dowling, S. (2013) *Cyber crime: a review of the evidence* (research report 75). London: Home Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf [Accessed 23 March 2022].

Min, C. & Shen, F. (2020) Grievances, resources, or values? Predicting online citizen-initiated government contacts in China. *Telematics and Informatics*, 56, 101479, pp.1–12.

Mumporeze, N. & Prieler, M. (2017) Gender digital divide in Rwanda: a qualitative analysis of socioeconomic factors. *Telematics and Informatics*, 34(7), 1285–1293.

Naegler, L. & Salman, S. (2016) Cultural criminology and gender consciousness: moving feminist theory from margin to center. *Feminist Criminology*, 11(4), 354–374.

Oakley, A. (2018) *From here to maternity (reissue): becoming a mother*. Croydon: Policy Press.

Office for National Statistics (2017a) *Changes to the Crime Survey for England and Wales*. London: HMSO.

Office for National Statistics (2017b) *Crime Survey for England and Wales, 2015–2016* [data collection]. UK Data Service. SN: 8140. Available at: http://doi.org/10.5255/UKDA-SN-8140-1 [Accessed 20 March 2022].

Öztürk, N. & Ayvaz, S. (2018) Sentiment analysis on Twitter: a text mining approach to the Syrian refugee crisis. *Telematics and Informatics*, 35(1), 136–147.

Painter, K. (1992) Different worlds: the spatial, temporal and social dimensions of female victimisation. In: Evans, D.J., Fyf, N.R. & Herbert, D.T. (Eds.) *Crime, policing and place: essays in environmental criminology*. Abingdon: Routledge.

Park, J., Cho, D., Lee, J.K. & Lee, B. (2019) The economics of cybercrime: the role of broadband and socioeconomic status. *ACM Transactions on Management Information Systems (TMIS)*, 10(4), 1–23.

Powell, A., Stratton, G. & Cameron, R. (2018) *Digital criminology: crime and justice in digital society*. Abingdon: Routledge.

Sabillon, R., Cavaller, V., Cano, J. & Serra-Ruiz, J. (2017) Cybercriminals, cyberattacks and cybercrime. In: *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*. Vancouver, BC., Canada: Institute of Electrical and Electronics Engineers (IEEE).

Sabon, L.C. (2018) Force, fraud, and coercion: what do they mean? A study of victimization experiences in a new destination Latino sex trafficking network. *Feminist Criminology*, 13(5), 456–476.

Shaari, A.H., Kamaluddin, M.R., Paizi, W.F. & Mohd, M. (2019) Online-dating romance scam in Malaysia: an analysis of online conversations between scammers and victims. *GEMA Online® Journal of Language Studies*, 19(1), 97–115.

Sharp, F.S. (2015) Feminist criminology and gender studies. *International Encyclopedia of the Social & Behavioral Sciences*, 2(8), 912–917.

Sherman, R.C., End, C., Kraan, E., Cole, A., Campbell, J., Birchmeier, Z. & Klausner, J. (2000) The Internet gender gap among college students: forgotten but not gone? *Cyberpsychology, Behavior, and Social Networking*, 3(5), 885–894.

Smith, W.R. & Torstensson, M. (1997) Gender differences in risk perception and neutralizing fear of crime: toward resolving the paradoxes. *British Journal of Criminology*, 37, 608–634.

Solano, P.C. & Peinado, A.J.R. (2017) Socio-economic factors in cybercrime: statistical study of the relation between socio-economic factors and cybercrime. In: *2017 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*. London: Institute of Electrical and Electronics Engineers (IEEE).

Stambolis-Ruhstorfer, M. & Tricou, J. (2017) Resisting 'gender theory' in France: a fulcrum for religious action in a secular society. In: Kuhar, R. & Paternotte, D. (Eds.) *Anti-gender campaigns in Europe*. London: Rowman & Littlefield.

Stavropoulos, V., Rennie, J., Morcos, M., Gomez, R. & Griffiths, M.D. (2021) Understanding the relationship between the Proteus effect, immersion, and gender among World of Warcraft players: an empirical survey study. *Behaviour & Information Technology*, 40(8), 821–836.

Steinmetz, K.F., Holt, T.J. & Holt, K.M. (2020) Decoding the binary: reconsidering the hacker subculture through a gendered lens. *Deviant Behavior*, 41(8), 936–948.

Stevens, F., Nurse, J.R. & Arief, B. (2021) Cyber stalking, cyber harassment, and adult mental health: a systematic review. *Cyberpsychology, Behavior, and Social Networking*, 24(6), 367–376.

Stylianou, S. (2003) Measuring crime seriousness perceptions: what have we learned and what else do we want to know. *Journal of Criminal Justice*, 31, 37–56.

Vella, K., Klarkowski, M., Turkay, S. & Johnson, D. (2020) Making friends in online games: gender differences and designing for greater social connectedness. *Behaviour & Information Technology*, 39(8), 917–934.

Walker, K. & Sleath, E. (2017) A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and Violent Behavior*, 36, 9–24.

Wang, V., Nnaji, H. & Jung, J. (2020) Internet banking in Nigeria: cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, 62, 100415, pp.1–11.

Watts, L.K., Wagner, J., Velasquez, B. & Behrens, P.I. (2017) Cyberbullying in higher education: a literature review. *Computers in Human Behavior*, 69, 268–274.

Whitty, M.T. & Buchanan, T. (2012) The online romance scam: a serious cybercrime. *Cyberpsychology, Behavior, and Social Networking*, 15(3), 181–183.

Yar, M. & Steinmetz, K.F. (2019) *Cybercrime and society*. London: SAGE.

How to cite this article: Lazarus, S., Button, M. & Kapend, R. (2022) Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice*, 1–18. https://doi.org/10.1111/hojo.12485