

**UUMILC 2017**  
**9<sup>TH</sup> UUM INTERNATIONAL LEGAL CONFERENCE**

**THE SCENT OF A WOMAN: GOVERNING THE GENDERED  
CRIME OF CYBER STALKING**

Wan Rosalili Wan Rosli (a)\*, Zaiton Hamin (b)  
\*Corresponding author

(a) Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia,  
rosalili@salam.uitm.edu.my

(b) Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia, zaihamin1@gmail.com

***Abstract***

Women have been the object of victimization for centuries and portrayed as the lesser sex in many cultures around the world. Crimes such as rape, domestic violence and stalking would predominantly happen to women. In the age of the Internet and borderless information, women have become the targeted sex with a high risk of victimization. Stalking, a crime that was once considered traditional have now transcend into cyberspace and fast becoming more dangerous and invasive than its conventional counterpart specifically in its harm and impact onto the victims. In the past decade, cyber stalking has escalated alarmingly and it is commonly committed by intimate partners and strangers alike; the gender-based commission by men and the victimization of women cannot be ignored. It is within this context that this paper seeks to examine the gendered nature of cyberstalking as a type of technology-facilitated violence against women in cyberspace. Importantly, the paper will also analyse the legal positions governing such crime in Malaysia. This article employs a doctrinal analysis using secondary data from the Penal Code, Communication and Multimedia Act 1998, law reports, academic journals, books, and online databases. The authors contend that women are the most vulnerable targets in cyberstalking victimization as the modus operandi of the crime is concealed by the shadow of anonymity and facilitated via trans-border connectivity. The Malaysian anti-stalking laws need to be urgently reviewed in order to sufficiently provide adequate protection and remedies to the victims of cyber stalking, particularly to women victims.

© 2018 Published by Future Academy [www.FutureAcademy.org.UK](http://www.FutureAcademy.org.UK)

**Keywords:** Cybercrime, Cyber Stalking, Stalking, Anti-Stalking laws, Victimization, Women.



## 1. Introduction

Stalking is an age-old crime that has been linked to delusional or erotomania and obsessive behaviours of people obsessing and following another person. In the early 20th century, stalking was identified as merely an obsessional behaviour or psychological rape (DeMatteo et al., 2017; Watson, 2017). From stalking of celebrities and public figures, the crime has also affected and changed the lives of ordinary people (Tjaden & Thoennes 1998). With the advent of information and communication technology and social networking platform in the last decade, cyber stalking emerged as a new threat to computer users (Spitberg & Cupach, 2007). The explosion of social media has created a new frontier in stalking behaviour. The digital environment provides stalkers additional avenues to commit their crimes. Traditional and cyber stalking are at a juncture where domestic violence was twenty years ago before it was classified as violence or crime against women. Such crime is considered as a type of gender-based crime that is primarily and exclusively committed against women. Since 1993, the UN Declaration on the Elimination of Violence against Women highlights that violence against women is an exhibition of the disparity of powers between males and females and that by social mechanisms, women are forced to take subordinate positions as compared to men. In 2006, Koffi Annan in this speech through the United Nations Development Fund for Women stated that violence against women and girls in the real world had become pandemic. The first part of this article contains the problem statement followed by the research question and the purpose of the study. The second part of this paper describes the research methodology engaged in conducting this research. Next is the findings of the study and the last section concludes the paper.

## 2. Problem Statement

Within the global context, since the late 1990s, the criminalisation of stalking and cyberstalking have begun in many jurisdictions around the world with the amendment of the traditional criminal laws. For instance, California became the first state in the USA to enact its anti-stalking law which provides better protection to female victims of cyber stalking and traditional stalking (Reyns, Henson, Fisher, 2011). Extant literature suggests women are most likely to be stalked rather than men. Godwin (2003) contends that in traditional stalking, it is mostly gender-motivated crime towards women and committed by men. King-Ries (2011) and Reyns & Englebrecht, (2014) also highlighted that woman is more vulnerable to be victims of cyber stalking rather than man. Medlin (2002), in his study, found that one out of 12 women (8.2 million) and one out of 45 men (2 million) in the United States had been stalked. The review of international studies indicates that women are more likely to be stalked rather than men and that females experience much fear due to stalking (Logan, 2010; Spitberg & Cupach, 2007; Sheridan & Lyndon, 2010). The extant literature in the USA, Australia, and the UK also shows that both traditional stalking and cyber stalking are gender-bias in which women are most likely to be stalked rather than men (Godwin, 2003, Medlin, 2002, Reyns, 2010; Nobles, 2013).

The literature in Malaysia on stalking and cyber stalking is rather scarce. The gendered nature of the crime has not been adequately addressed by the Malaysian law. However, the available recent literature seems to indicate the unwillingness of female victims of cyber stalking to report the crime to the

polic (Haron, 2010). Similarly, Cybersecurity Malaysia (2010) states that the problem of cyberstalking is merely on the tip of the iceberg because the actual number of cyberstalking victims may be higher and not all victims are willing to come forward to report to the police. The severe nature of the threat of cyber stalking which must not be taken lightly, have also been documented (The Star, 2010). Foong (2014) highlighted that Malaysia should follow the Singaporean counterpart in enacting specific anti-stalking laws to provide legal protection towards the victims adequately. The literature on the legislative response to such crime suggests that computer-specific law such as the Communications and Multimedia Act 1998 (from now on 'the CMA') may be the answer in prosecuting cyber stalking and cyber harassment in Malaysia (Hamin and Wan Rosli, 2016). Hence, there appears to be the lacuna in the literature on the extent to which the existing traditional and the cyber law may apply to govern cyber stalking in Malaysia. Given such a lacuna in the literature, this paper aims at examining the current legal position governing cyber stalking in Malaysia and intends to fill in such gap in the literature.

### **3. Research Questions**

The questions this research aims to address are as follows: Firstly, to what extent does the Communication and Multimedia Act 1998 and the Penal Code in Malaysia criminalise cyber stalking which appears to target women as victims? Secondly, in what manner could the anti-stalking legal framework in Malaysia be reformed to provide adequate protection to cyber stalking victims comprehensively?

### **4. Purpose of the Study**

The primary objectives of this paper are two-fold and as below: Firstly, to examine the extent to which the Communication and Multimedia Act 1998 and the Penal Code in Malaysia are criminalising cyber stalking which would target women as victims. Secondly, to propose for the reformation of the anti-stalking legal framework in Malaysia so as to provide adequate protection to cyber stalking victims comprehensively.

### **5. Research Methods**

This study adopts a qualitative methodology using library-based research method to critically review the literature on cyber stalking and traditional stalking particularly on the gendered nature of the crime. The primary and secondary sources of data will be examined through the content analysis method. The former relates to the Penal Code and the Communications and Multimedia Act 1998 upon which a critical review will be conducted to examine the legal framework of cyber stalking in Malaysia. The latter refers to the content analysis of textbooks, journal articles, government reports, working papers, commentaries on case laws and online databases such as Emerald, Hein Online and Sage Publication which is done to support the primary sources of data.

## 6. Findings

The research findings of this paper are as follows:

### 6.1. The Nature of Stalking and Cyber Stalking

Since the advent of information technology and the Internet, several crimes such as stalking has been increasingly prevalent worldwide (Woodlock, 2016, Ahlgrim, 2015, Walklate, 2003, Lamplugh, 2003). Stalking is defined as a repeated and unwanted pursuit that causes fear to another person. For instance, the early literature describes stalking as harassing or threatening behaviour that is repetitive and creating a threat to an individual (Thomas, 1993). More recent research shows that the nature of the offence remains the same. For example, the Modena Group on Stalking (2007) states that stalking is a phenomenon characterized by a variety of different behaviours which makes the analysis of the causes of such violence rather difficult. The most recent literature on stalking also indicates the unchanging nature of the crime. Heinrich (2015) contends that stalking is a type of harassment involving some persistent threats or putting in fear to the victim. Similarly, Brady and Bouffard (2015) suggest that stalking is a repeated variety of behaviours directed to another individual which causes reasonable fear to the victim. In Australia, criminal stalking is defined as a conduct intentionally directed at a person repeatedly and involving specific acts such as contacting a person through email, phone, fax, electronic mail or through any other technology (Reyns, 2010).

The literature on cyber stalking indicates that cyber stalkers harass victims by using technological means such as sending threats via the Internet, harming the victim's reputation or 'smearing' through the social media, causing damage to data or attempt to access confidential information on the victims (Bocij, 2003, Vasiiu and Vasiiu, 2013). Cyber stalking also covers activities such as bullying, harassment, defaming and threatening (Bocij, 2003; Aa, 2011). The more recent literature on such crime suggests that cyber stalking is a collection of behaviours conducted through technology such as e-mail, forums, blogs and social networking websites. The perpetrator repeatedly harasses and pursue the victim, by making threats, accusations, monitoring and also impersonation, which causes alarm or fear in such victim (Mutawa et al., 2016). Cyberstalking has been defined as inappropriate, unwanted social exchange behaviours initiated by a perpetrator via online or wireless communication technology and devices (Heinrich, 2015, Piotrowski, 2012). Cyberstalking may be more dangerous and common than traditional stalking as the ICT including the Internet are providing tremendous opportunities to target any victims around the world (Brady and Nobles, 2015, Aa, 2011). The fact that the crime is technology-enabled and the difficulty in detecting the offender have made it easier for the cyber stalkers to conceal their identities, alter critical data, move and delete information quickly and destroy the evidence (Aa, 2011).

The extent of cyberstalking is becoming more imminent and more severe around the world (Bocij & Mcfarlane, 2002). It is estimated that about 20 percent to 40 percent of Internet users are victimized through cyber stalking (Tokunaga and Aune, 2015). In 2007, cyber stalking victims ranged from 474,000 to 18.7 million across the globe, and the current number is unknown due to flawed and outdated statistics (Aa, 2011). In Australia, 98 percent of the domestic violence victims have also experienced cyber stalking (Rawlinson, 2015). More than 38 percent of cyberstalking victims fears that the offensive behaviour of the offender online would develop into a face-to-face confrontation (Al-Khateeb and Epiphaniou, 2016).

The duration of the crime which the victims may have to endure may be quite long. For instance, Paladin (2014) contends that more than 42 percent of victims of stalking and cyberstalking are being stalked for more than 24 months. That the victims of cyber stalking may have prior relationships that ended bitterly with the offender are also documented (Mishra and Mishra, 2008, Valentine, 2001), and in 45 percent of all cases, the offenders are usually ex-partners (National Stalking Helpline, 2015).

## **6.2.Cyber Stalking and Women Victimization**

The extant literature indicates that stalking is gendered in nature as the majority of stalking victims are women and the majority of the perpetrators are men (DeMatteo et al., 2017; Godwin, 2003; King-Ries, 2001; Reyns & Englebrecth, 2014; Aa, 2012; Strategy and Policy Directorate research team, 2014, National White-Collar Crime Centre, 2013). Furthermore, the available statistics indicate that women have a higher level of victimisation of such crime than men. For example, early figures in 1998 found that women are three to four times more likely to be the targets of stalking rather than man (National Violence Against Women Survey, 1998). In the USA, one out of 12 females (8.2 million) and one out of 45 male (2 million) had been stalked (Medlin, 2002). Recent reports indicate the status quo in female victimization for cyber stalking. For instance, in 2011 the National Stalking Helpline statistics show that the majority of cyberstalking victims are women (80 percent) and the majority of perpetrators are male (70.5 percent). Patel (2013) contends that majority of victims are female (80.4 percent), and the majority of offenders are male (70.5 percent). The most recent figure from the British Office for National Statistics (2015) reported that in 2014 to 2015, twice as many women rather than men said having experienced stalking which is more than 1.4 million female victims. The age of the majority of the victims appears to be less than 30. For instance, in England and Wales, women aged between 16 years old to 19 years old and aged between 20 years old to 24 years old are more likely to be victims of stalking compared to other age groups (British Office for National Statistics, 2015). In Australia, the Australian Bureau of Statistics reported that one in every five women above the age of 15 years had been stalked (Australian Bureau of Statistics, 2006).

The rationale for the tendency for such gendered victimization of women may be because women tend to spend more time online (Heinrich, 2015). However, the percentage of the actual stalking victims is not very accurate as there is no proper data on victims of stalking and cyberstalking are made available (Mutawa et al., 2016). The literature suggests that cyber stalking may have a substantial impact on the victims. The high prevalence of such crime may lead to many strains in the victims' personal and professional life. Such issues may range from personality changes, insomnia, post-traumatic stress disorder (PTSD) and other psychiatric and psychological complaints (Watson, 2017; Bocij & Mcfarlane, 2002; Aa, 2011; Maple, Short, and Brown, 2011; Middlemiss, 2014). It is reported that thirty percent of female victims sought psychological counselling, almost 7 per cent of victims does not return to work. Eleven percent of women victims relocated to another place and changed their identities to protect themselves and their loved ones, as a result of stalking and cyberstalking (Aa, 2011).

### **6.3.Lack of Specific Legal Provision in Malaysia**

In Malaysia, several laws could be used to prosecute stalkers and cyber stalkers. The traditional criminal law such as the Penal Code and computer-specific law such as the Communications and Multimedia Act 1998 (CMA 1998) contain provisions that may be suitable to prosecute stalking and cyber stalking offenders. Section 503 and section 506 may accommodate stalking, and cyber stalking as both sections cover criminal intimidation. Criminal intimidation under section 503 is when a person threatens another with any injury to his person with the intent to cause alarm to that person. The punishment for such crime under section 506 is incarceration for a term that may extend to two years or fine or both. To date, there are about eleven reported decisions on criminal intimidation. However, none of these cases involved stalking or cyber stalking. Rather, cases commonly prosecuted under section 503 included threatening the victim with a parang to instil fear into the victim (*Sinnasamy A/L Kaliappan v PP* (2005) MLJU). Another case includes putting in fear of injury towards the victim if the victim failed to pay the money demanded by the accused (*Abdul Wahab bin Mohd Noor v PP* (1993) MLJU 331)

Section 351 on criminal assault and section 354 on assault or criminal use of force to a person with intent to outrage modesty may be applicable in prosecuting stalking and cyber stalking. If found guilty, the offender shall be punished with imprisonment for a term which may extend to ten years or fine or whipping or with any two such punishments. To date, there are about forty-seven reported cases under section 354. Two examples of such situations are *PP v HAHS* (2012) 8 MLJ 109 which concern the outrage of modesty of a 12-year-old girl by an accused who was an Imam. The case of *Mohd Hanafi Bin Ramly v PP* (2011) MLJU 475 involved outraging the modesty of the victim by kissing her on the cheek. However, nobody has been prosecuted for stalking or cyberstalking under sections 351 or 354.

Section 233 of the CMA 1998 may be available to prosecute cyberstalking cases. Such provision covers the improper use of network facilities or network services. Section 233(1)(a) involves continuous and repeated acts and behaviours carried out by means of any network facilities, network services or applications to make, solicits or initiate the transmission of any comments, suggestions or other communication which is obscene, indecent, false, menacing or offensive with the intent to annoy, abuse, threaten or harass another person. Section 233(1) (b) further provides that a person who initiates communication by using application services whether continuously or repeatedly, without disclosing his identity with the intention to annoy, abuse, threaten and harass any person at any number or electronic address may be found guilty under the said section. A person who commits an offence under this section shall on conviction be liable to a fine not exceeding fifty thousand ringgit or imprisonment for a term not exceeding one year or both (Section 233(3) of the CMA 1998). A person can also be further fined for one thousand ringgit for every day during which the offence continued after the conviction (Section 233(3) CMA 1998). Despite the possibility of using section 233 to prosecute the perpetrators for cyber stalking, up until today, no such case has been brought before the court. The only case that has been prosecuted under section 233 of the CMA 1998 is the case of *Rutinin b Suhaimin v PP* (2014) 5 MLJ 282 whereby the accused had published a comment via his internet account that “Sultan Perak sudah gila!!!!!!” However, the decision was overturned as there was evidence that anyone can access the defendant's account as his computer and his Internet account was accessible by other persons and on the day mentioned in the charge and that his IP line was on continuous login from the 8 am to past 7 pm.

A recent case in 2013 involving cyber stalking by a female perpetrator against her former boyfriend indicates a missed opportunity for the Malaysian court to decide on such crime as the case was brought by the victim on the ground of cyber defamation (*David Clayworth v Lee Chiang Yan*, 2013 (Unreported)). Since 2010, after the break-up of her relationship with her boyfriend, Lee Chiang Yan, a Malaysian, relentlessly cyber stalked Lee David Clayworth, a Canadian teacher. The accused posted numerous false posting on the Internet and some of which contained nude pictures of him with a caption 'Genital herpes' The defendant also took over the victim's email and skype accounts and posted messages that the victim was a child molester, paedophile and preferred having sex with his students. The victim sued the defendant for defamation and won the case. The court ordered the defendant to pay RM66, 000 for damages. However, the online assault did not stop even after a contempt of court order was issued against her. The defendant had since fled the country to live in Australia. The victim's requests to the search engines to remove his name from the search engines were futile as they merely ignored his requests. Had the case been dealt with through the criminal law avenue and on a charge of cyberstalking, perhaps the court would have the opportunity to apply either the traditional criminal law or the cyber law to decide this case.

Another controversial case involving a female victim is a Singaporean case of Colin Mak Yew Loong who stalked an American Opera singer, Leandra Ramm since 2005 after he saw her performed on television (*PP v Colin Mak Yew Loong*, 2013 (Unreported)). He sent her threatening e-mails and voice messages for more than six years, which included threats of personal violence. The accused was charged for criminal intimidation under sections 503 and 506 of the Singapore Penal Code and was sentenced to three years of imprisonment and SD5000 fine. This case occurred before the creation of the Protection from Harassment Act 2014 (PHA 2014) in Singapore. If the case were to happen and be decided in Malaysia, the same provisions would apply as the said criminal intimidation provisions in Singapore is in parimateria with section 503 of the Malaysian Penal Code. However, if the case were decided post-PHA 2014, the accused would have been charged with cyberstalking under section 7 of the PHA 2014, which on conviction, the accused can be liable to a fine not exceeding SG\$5,000 and imprisonment not exceeding twelve months or both (PHA 2014). If the harassment towards the victim continues after the conviction, the accused may also be charged with the subsequent offence(s) and may be liable to a fine not exceeding \$10,000 and an imprisonment for a term not exceeding two years or both.

#### **6.4.Reforming the Anti-stalking laws in Malaysia**

The Malaysian legal framework demonstrates that there is a deficiency in the law of cyber stalking, be it under the Penal Code or the CMA 1998, as there is no specific provision to cover the real world stalking or cyberstalking. Be that as it may, any incidence of such crime may be prosecuted for criminal intimidation or assault under the Penal Code or Section 233 of the CMA 1998 discussed above. Despite the deterrent utility of these provisions in punishing the offender, such provisions lack any legal protection for female victims, including the physical protection for the victim, restraining the stalker from coming into contact with the victim, or stopping the perpetrator from committing further stalking against the victim. Given the lack of protection for female victims of stalking and cyberstalking in Malaysia, there is a dire need for the existing traditional law to be reformed to include the provision of a protection

order, restraining order and injunction along the lines of those orders provided in the Domestic Violence Act 1994. In this context, Malaysia should create several provisions in the existing Penal Code to include the particular substantive law and the penalty for cyber stalking. Beyond this scope, the procedural law should also be created to include the orders that would allow the court to make in any cyber stalking cases. Alternatively, a legislative mechanism may be designed to establish a new anti-stalking law modelled on the Protection from Harassment Act (PHA) 1997 in England and Wales with distinct provisions for stalking in Section 2A & Section 4A. Similar to the PHA 1997, any female victim in Malaysia could be well protected from further harassment with the available remedies such as injunctions, protection orders, and restraining orders. Whatever the right model that is adopted by the anti-stalking law in Malaysia and regardless of the gendered nature of such crime, such law should be technology-neutral and gender-neutral to cater for all types of stalking and to protect all victims irrespective of their gender.

## 7. Conclusion

In the last two decades, the threats of the real-world stalking and cyber stalking have become more prevalent than ever before. However, the concern by many people of such crime is the gendered nature of the offence in which women are usually the victim of such offences. More often than not, there seems to be a prior relationship between the stalkers and the female victims. The fact that in Malaysia no prosecution has been brought before the courts on such crimes compounded the problem of the applicability of the traditional criminal law and the cyber law to such offences. Having said that, due to the persistent and hidden nature of cyberstalking and the enormous impact on the victims, such victims deserve more legal protection than what is currently available, regardless of their gender. Despite the common gendered nature of cyber stalking, the anti-cyber stalking legislation should not be gender-bias and should cover any victim. What is significant is that the Malaysian legal framework on stalking and cyber stalking is in dire need of an immediate review so that new provisions or a new law could be created to provide adequate protection and remedies such as protection orders and restraining orders to the victims of cyber stalking and for women victims. The experiences of specific anti-stalking laws in England and Wales and also in Singapore would be good lessons for Malaysia to learn and benchmark. Significantly, comparative analysis between the Malaysian laws and that in England and Wales may serve as an implication for future research on such crime.

## Acknowledgments

This work was supported by research grant FRGS/1/2016/SSII0/UITM/02/5 by the Research Management Centre, UiTM Shah Alam, Selangor.

## References

- Aa, S. (2011). International (cyber) stalking. In R. M. Letschert, & J. J. M. van Dijk (Eds.) *The new faces of victimhood: globalization, transnational crimes and victim rights*. Netherlands: Springer Science & Business Media. (pp. 191-213).
- Al-Khateeb, H., Epiphaniou, G. (2016). How technology can mitigate and counteract cyber stalking and online grooming. *Computer & Security Journal*, 14-18.



- Bocij, P., McFarlane, L. (2002). Cyberstalking: Genuine problem or public hysteria? *Prison Service Journal*, 140, 32-35.
- Brady, P., Bouffard, L. (2015). *Majoring in stalking: Exploring stalking experiences between college students and the general public*. Crime Victims' Institute, Sam Houston State University. Retrieved from <http://dev.cjcenter.org/files/cvi/Stalking%20Series3tlnpdf.pdf>.
- Brady, P., Nobles, M., R. (2015). The dark figure of stalking: Examining law enforcement response. *Journal of Interpersonal Violence*, 1-25.
- Bocij, P. (2003). Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet. *First Monday*. Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1086/>
- Cybersecurity Malaysia. (2010). *Cyberstalking a serious threat*. Retrieved from [http://cybersecurity.my/en/knowledge\\_bank/news/2010/main/detail/1853/index.html](http://cybersecurity.my/en/knowledge_bank/news/2010/main/detail/1853/index.html)
- DeMatteo, D., Wagage, S., Fairfax-Columbo, J. (2017). Cyberstalking: Are we on the same (web) page? A comparison of statutes, case law and public perception. *Journal of Aggression, Conflict and Peace Research*, 9(2), 83-94.
- Godwin, M. (2003). *Cyber rights: Defending free speech in the digital age*. Cambridge: The MIT Press.
- Hamin, Z., Wan Rosli, W, R. (2016, September 28-29). *Managing the risk of cyber harassment @ work*. Paper presented at the 8<sup>th</sup> International Management and Accounting Conference (IMAC8), Adya Hotel. Langkawi Island, Malaysia.
- Haron, H., Yusof, F. (2010). *Cyber stalking: the social impact of social networking technology*. Paper presented at the International Conference on Education and Management Technology (ICEMT 2010). Cairo, Egypt.
- Heinrich, P., A. (2015). Generation iStalk: An examination of the prior relationship between victim of stalking and offenders. *Theses, Dissertations and Capstones*, Paper 917.
- King-Ries, A. (2011). Teens, technology, and cyber stalking: The domestic violence wave of the future? *Texas Journal of Women and the Law*, 20(2), 131 – 164.
- Maple, C., Short, E., Brown, A. (2011). *Cyberstalking in the United Kingdom*. National Centre of Cyberstalking Research. Retrieved from [https://www.beds.ac.uk/\\_data/assets/pdf\\_file/0003/83109/ECHO\\_Pilot\\_Final.pdf](https://www.beds.ac.uk/_data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf).
- Medlin, N. (2002). *Stalking to cyber stalking, a problem caused by the internet, law and the internet*. Georgia State University College of Law. Retrieved from <http://gsulaw.gsu.edu/lawand/papers/fa02/medlin/>
- Middlemiss, S. (2014). Let the stalker beware? Analysis of the law of stalking in Scotland. *The Journal of Criminal Law*, 78 JCL, 407-422.
- Mishra, A., Mishra, D. (2008). Cyber stalking: A challenge for web security. *Cyber Warfare and Cyber Terrorism*.
- Mutawa, N., Bryce, J., Fanqueira, V., Marrington, A. (2016). Forensic investigation of cyberstalking cases using behavioural evidence analysis. *Digital Investigation*, 16, 96-103.
- National White-Collar Crime Centre. (2013). *Cyberstalking*. NW3C, Inc. Retrieved from: <http://www.nw3c.org/docs/research/cyberstalking>
- Office for National Statistics. (2015). *Chapter 4: Violent crime and sexual offences – Intimate personal violence and serious sexual assault*. Retrieved from <http://www.crimesurvey.co.uk/>.
- Paladin (2014). *Stalking and harassment – A shorthand guide about digital and cyberstalking*. Retrieved from <http://paladinservice.co.uk/wp-content/uploads/2014/11/Digital-and-Cyber-Stalking-Toolkit-2013.pdf>.
- Piotrowski, C., (2012). From workplace bullying to cyberbullying: The enigma of e-harassment in modern organizations. *Organization Development Journal*, 3 (4).
- Rawlinson, C. (2015). *Cyber stalking increasing, 'easy' way to abuse women: Domestic violence report*. Domestic Violence Resource Centre of Victoria in 774 ABC Melbourne.
- Reyns, B. (2010). *Being pursued online: Extent and nature of cyberstalking victimization from a lifestyle/routine activity perspective* (Unpublished Doctoral Thesis). University of Cincinnati. Retrieved from [https://etd.ohiolink.edu/pg\\_10?0::NO:10:P10\\_ACCESSION\\_NUM:ucin1273840781](https://etd.ohiolink.edu/pg_10?0::NO:10:P10_ACCESSION_NUM:ucin1273840781)
- Reyns, B., Henson, B., Fisher, B., (2011). Applying cyberlifestyle-routine activities theory to cyber stalking victimization. *Criminal and Justice Behaviour*, 38.
- Reyns, B.,W., Englebrecht, C., M. (2014). The fear factor: Exploring predictors of fear among stalking victims throughout the stalking encounter. *Journal of Crime & Delinquency*, 59(5), 788-808.
- Spitzberg, B., H, Cupach, W., R. (2007). The state of the art of stalking: Taking stock of the emerging literature. *Aggression and Violent Behaviour*, 12, 64–86.

- Thomas, K.,R. (1993). How to stop the stalker: State anti- stalking laws. *Criminal Law Bulletin*, 29, (2), 124-136.
- Tokunaga, S., Aune, K. (2015). Cyber defense: A taxonomy of tactics for managing cyberstalking. *Journal of Interpersonal Violence*, 1-25.
- Vasiu, I., Vasiu, L. (2013). Cyberstalking nature and response recommendations. *Academic Journal of Interdisciplinary Studies*, 2(5), 226-234.
- Watson, J., C. (2017). *Cyberstalking and women: The perception of threat between two different age groups of women* (Unpublished Doctoral Dissertation), Alliant International University. Retrieved from <https://search.proquest.com/docview/1845003135?pq-origsite=gscholar>.
- Woodlock, D. (2016). The abuse of technology in domestic violence and stalking. *Violence Against Women*, 1-1.