International Journal of Emerging Trends in Social Sciences
ISSN: 2521-3539
Vol. 4, No. 2, pp. 58-66, 2018
DOI: 10.20448/2001.42.58.66

OVIAR: Towards a Model for Cyberstalking Intervention and Reduction

Paul Bocij[1]

[1]Aston University , England.
Email: paulbocij@gmail.com

Abstract

Despite more than two decades of research, relatively little is known about cyber stalking and similar phenomena. In particular, the existing literature tells us little about how cases unfold, how they can be managed or how we can work towards reduction. This paper presents a model depicting the dynamics and lifecycle of a cyber stalking episode. While primarily concerned with cyberstalking, the model may also be relevant to other forms of victimisation and is accordingly titled the Online Victimisation Intervention & Reduction (OVIAR) Model. Cyberstalking is shown as an iterative cycle made up of discrete stages. It is argued that each stage provides opportunities to deter the cyberstalker allowing the model to offer guidance about which interventions may be effective at a given point in the lifecycle. In proposing the model, the work draws upon a number of areas including information systems, criminology and psychology. A key part of the discussion involves the decision behaviour of the cyberstalker. It is argued that cyberstalking incidents involve a number of decision points that may serve to curtail or escalate the cyberstalker's activities. The decisions made by the cyberstalker will be influenced by several factors, including the feedback he receives from his actions. Understanding how cyberstalkers make decisions can provide opportunities to prevent discourage further acts of harassment against victims. It may also benefit attempts to reduce or prevent victimisation in the first place. In discussing these areas, we draw upon areas such as rational choice theory, victim coping responses and the notions of intrinsic and extrinsic feedback.The model is intended to be understandable by a wide range of stakeholders, including law enforcement, technology professionals and victims themselves. For those involved in dealing with cyberstalking, it provides a tool that can be used to inform the management of cases. For academics, it is intended to provide a framework for further discussion and research.

Keywords:
OVIAR
Model
Lifecycle
Cyberstalking
Online victimisation
Online harassment.

Publisher:
Scientific Publishing Institute

1. Introduction

This paper describes the OVIAR model in depth. Its focus is on the use of the model as an explanatory tool and its application as a means of mitigating harassment. Some of the research that informed the development of the model will appear in one or more sister papers (in preparation).

The work adopts a number of conventions for stylistic purposes and in order to aid understanding. For the purposes of the discussion provided here, cyberstalking is defined as:

> A group of behaviors in which an individual, group of individuals or organization uses information and communications technology to harass another individual, group of individuals or an organization. Such behaviors may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring, the solicitation of minors for sexual purposes, and any form of aggression.

> Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress. (Bocij, 2004).

This definition has been adopted since it is considered well-established, comprehensive and clear. It can also be argued that the definition encompasses a wide range of deviant or antisocial behaviours found online. This means that much of what is discussed, including the model proposed later on, is likely to apply to similar phenomena, such as cyberbullying.

Many of those working in the field refer to those pursued by cyberstalkers as *targets*. It is felt that this dehumanises those suffering harassment, effectively reducing them to objects. In this paper those experiencing cyberstalking are referred to as *victims* in order to emphasise the very real harm that they suffer.

The paper also considers there to be a distinction between stalking and cyberstalking. *Stalking* largely takes place in the physical world and is sometimes termed offline stalking. *Cyberstalking* predominantly takes place online and can have characteristics or behaviours not commonly seen in offline stalking. Serial cyberstalking, for instance, can involve one or more cyberstalkers pursuing a number of different victims simultaneously or a number of victims sequentially over relatively short timescales. Cases of cyberstalking may spill over into the physical world and vice versa. We draw a hazy dividing line based on where the victimisation first started, where most of the harassment takes place and the actions of the harasser. In this way, for example, a case of stalking may evolve into cyberstalking if the harasser shifts most of his activities online or if he takes part in group or serial cyberstalking.

Victims of cyberstalking are referred to as females while cyberstalkers are referred to as males. This convention is adopted for stylistic purposes but also reflects the reality of stalking and cyberstalking, where a number of studies have reported that females represent the largest proportion of victims and males represent the largest proportion of cyberstalkers (Bocij, 2004; Dressing, Bailer, Anders, Wagner, & Gallas, 2014; Jaishankar, 2011; Reyns, Henson, & Fisher, 2012).

2. The Online Victimisation Intervention & Reduction (OVIAR) Model

The Online Victimisation Intervention and Reduction (OVIAR) Model depicts the progression of what might be considered a "typical" episode of cyberstalking, though it is recognised that every case is likely to have unique elements. It is felt that cyberstalking episodes tend to unfold in a similar way irrespective of their severity. A case involving threats or other online abusive behaviour is likely to follow the same basic pattern as one that ends in a physical attack.

It should be stressed that this model is not intended to be seen as a perfect representation of how cyberstalking episodes unfold. It is presented here with the intent of stimulating discussion and encouraging further research. The approach taken means that the model can be extended easily. It is also possible to decompose each stage further, enabling more detail to be added as necessary. It is hoped that others will use the material offered here as scaffolding for the creation of a more sophisticated and effective tool.

One of main purposes of the model is to identify points where specific interventions are likely to be most effective and where they are likely to be unsuccessful. It is also intended to provide academics, law-enforcement and others with a simple tool that can be used for a number of purposes, from planning research to identifying where to focus resources.

Although the model is aligned with the definition of cyberstalking given earlier, this does not mean it cannot be applied more widely. Thus, it may be of some use in investigating other forms of victimisation, both online and offline, such as bullying or cyberbullying. For this reason, the title of the model refers to online victimisation rather than cyberstalking. However, it should be noted that the model is likely to be of limited use in examining atypical cases of harassment, such as group cyberstalking or corporate cyberstalking. Furthermore, some elements of the model may be less applicable to cases where the cyberstalker is an ex-intimate rather than a stranger.

The structure of the model draws upon Herbert Simon's classic model of decision making (Radford, 2013). While an extended discussion of rational decision making is beyond the scope of this paper, it is worth highlighting some of the main reasons why Simon's model is considered particularly useful in the context of cyberstalking.

First, Simon's model is relatively simple to understand, making it widely accessible. In turn, this is likely to make the OVIAR model easier to comprehend and use effectively by those without specialist knowledge, including the victims themselves, law enforcement and support organisations. In addition, since many people will already be familiar with Simon's model they should be able to grasp its use within a new context quite easily.

Second, Simon's model portrays the decision making process as a deliberate course of action intended to achieve a specific result. It is felt that its use will help to reinforce the view that cyberstalkers consciously set out to victimise others and that unintentional cyberstalking is very rare. In the offline world, cases where the stalker does not have a prior relationship with the victim are uncommon and are often described in terms of stranger stalking. Such cases often involve stalkers who are trying to establish a romantic relationship with the victim and are classed as *intimacy seekers* or *incompetent suitors* by writers such as Mullen, Pathé, and Purcell

(2008). However, in the online world stranger cyberstalking is more common (Glass, 2006; Kirwan, 2011) with various estimates suggesting it makes up more than 40% of all cases (Dempsey, 2010; B. S. Fisher & Sloan, 2013; Reyns et al., 2012). In many of these cases the cyberstalker may not have even the most basic information about the victim, such as her gender (Bocij & McFarlane, 2003) so is unlikely to be an intimacy seeker or incompetent suitor. Instead, he is more likely to be following a deliberate course of action with the aim of causing distress or other harm to the victim.

Third, Simon's model fits well with how cyberstalking incidents typically unfold and seems to provide an effective means of depicting the mechanics of harassment accurately.

Finally, modern variations on the Simon's model have introduced the idea of iteration, where key activities are repeated until a decision is reached or the problem being dealt with is solved. As an example, Bocij, Greasley, and Hickie (2015) describe a version of the model that includes an evaluation stage, where the decision maker determines if the actions taken so far have resolved the problem. If the problem has not been solved, the decision maker returns to the start of the process and begins another cycle. As discussed later, the idea of iteration is important when considering the repetitive behaviours typically seen in cyberstalking cases.

The role of repetition also fits well with criminological models of crime and deviant behaviour. It can be argued, for instance, that the iteration shown in the model transforms a cyberstalker's behaviour into a routine activity. This seems reasonable given that a number of studies have connected online victimisation with Routine Activity Theory (see, for instance, (Choi & Lee, 2017; Hawdon, Costello, Ratliff, Hall, & Middleton, 2017; Leukfeldt & Yar, 2016; Pyrooz, Decker, & Moule, 2013). As an example Näsi, Räsänen, Kaakinen, Keipi, and Oksanen (2016) conducted a study that attempted to predict online victimisation in a group of 3,565 young people aged 15 – 30. The study used representative samples from the USA, Finland, Germany, and the UK. The work concluded that "…routine activity theory is a useful tool for predicting online victimization" (Näsi et al., 2016) though its value varied across countries.

Figure 1. Shows the OVIAR model and how a set of core behaviours are repeated over time.

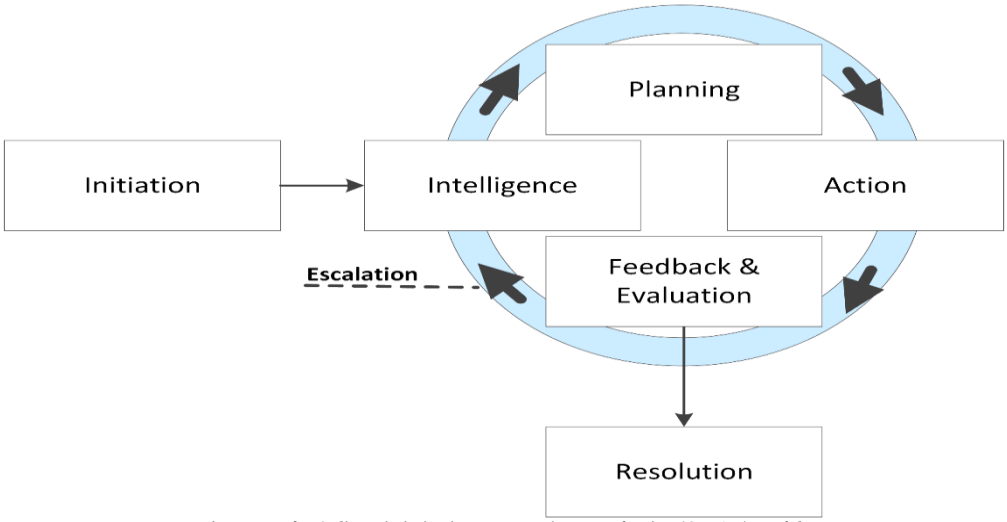

Figure-1. The Online Victimisation Intervention & Reduction (OVIAR) Model.

As can be seen, the model is made up of five major stages. A description of each stage and additional comments follow.

In the *Initiation* stage, two events take place: the victim first comes to the cyberstalker's attention and the cyberstalker makes the decision to pursue her.

It is often possible to identify a single *trigger event* that results in an episode of cyberstalking. In many cases, the trigger event may be insignificant to the victim or outside observers but of great importance to the cyberstalker. The trigger event may be so trivial that the victim is unable to identify it as such. As an example, Bocij (2005) recounts a case where the victim's accidental misuse of a single technical term in a post to a message board resulted in a prolonged campaign of harassment against her by an organised group of cyberstalkers. The group saw the misuse of the word as the final evidence needed to prove that the victim was part of a conspiracy against them.

In many cases, identifying the trigger event will be relatively simple. Many cases of stalking and cyberstalking begin when a relationship ends. In such cases, the trigger event might take the form of one partner moving out of the shared home, or when legal documents finalising the breakup are received.

The *Intelligence* stage involves the cyberstalker collecting information about the victim in order to plan his actions. The more information he is able to find, the more possibilities become available to him in terms of actions he might take against the victim.

The information gathering process will often be unstructured and informal, perhaps involving little more than the use of search engines and other publicly available tools. Sometimes, however, a much more deliberate and organised approach might be taken. Cyberstalkers may go to great lengths to collect information using both legal and illegal means, often using technology to aid them (King-Ries, 2011). A good example is the use of spyware to monitor the victim's computer or mobile phone. Such software is inexpensive (even free), easily available and relatively simple to install. Once active, the software can capture every piece of information moving in or out of the infected device, from webcam images to individual keystrokes that might reveal passwords or other sensitive data. Magnet & Gates discuss the use of spyware in the context of cyberstalking:

> Such computer programs may be covertly installed. Once set up, the software gives the installer second-by-second screen shots of what is happening on the computer that carries the spyware, which in turn can be emailed to the stalker's computer or cell phone. Information transmitted may include email messages or communication sent by an Internet phone. In this way, every moment of the target's day may be tracked — including, for example, email sent to a domestic violence shelter or a call made to a crisis hotline.
> (Magnet & Gates, 2013).

The *Planning* stage is where the cyberstalker selects the action he wishes to take. As already mentioned, the choice of possible actions may be constrained by a lack of information about the victim. There may also be a range of other factors that limit the cyberstalker's actions, such as a lack of resources or a lack of technical knowledge. Additional factors might include the fear of being caught, time pressures and the amount of effort needed to carry out a given action.

In the *Action* stage, the cyberstalker carries out his plan. At this stage he may also attempt to gather information that can be used to adjust his actions in response to the victim's reactions.

In the *Feedback & Evaluation* stage, the cyberstalker assesses the results of his actions. In general, feedback can be obtained very quickly providing the near-instant gratification that cyberstalkers and other deviants crave (Daynes, 2012; Hazelwood & Burgess, 2009; Lipsey & Landenberger, 2006).

It is here that an important decision point is reached. Bocij (2003) argues that cyberstalkers are likely to find that feedback received online is less rewarding and less enjoyable than that obtained first-hand. This may result in several possible outcomes. If the feedback received is satisfactory, the cyberstalker may continue his pursuit of the victim by repeating the behaviours he sees as having been successful or by experimenting with new behaviours. If the feedback received is unsatisfactory, he may lose interest in the current victim and select a new one. However, there is also the possibility that the cyberstalker may escalate his pursuit of the victim in order to obtain the reaction he desires. This escalation might take the form of more frequent or more extreme acts of harassment and may move from the online world into the physical world. The possibility of such escalation is shown in Figure 1 by a dotted line.

There is no research to provide guidance about the role of feedback and how it may affect the risk of a cyberstalker turning towards more extreme acts of harassment. Put simply, while it seems reasonable to assume that showing no reaction to acts of harassment is likely to discourage a cyberstalker, there appears to be no concrete research evidence to support this.

Many experts advise not responding to cyberstalkers but victims often receive conflicting messages. This is because some legislation dealing with cyberstalking requires that the contact between the victim and cyberstalker is "unconsented". This is often interpreted as meaning that the victim needs to contact the cyberstalker and tell him to stop his behaviour before legal intervention becomes possible. However, this can be problematic since "Any kind of interaction can be psychologically rewarding for the pursuer. He or she might believe that any kind of contact is positive" (National Centre for Cyberstalking Research, 2015). Despite this warning, the National Centre for Cyberstalking Research and others (e.g. (Donovan & Bernier, 2009; Miller, 2008; Pathé, 2002; Wang, 2006)) still advise victims to contact cyberstalkers to make it clear that they want no further interaction. The issue of "unconsented" contact has been discussed a number of times (e.g. (DeMatteo, Wagage, & Fairfax-Columbo, 2017; Haider & Jaishankar, 2009; Hazelwoode & Koon-Magnin, 2013; Pinals, 2007)) since it was first raised by Bocij and McFarlane (2002) at the turn of the century, so it is not considered further here. However, the broader question of how feedback may encourage or discourage cyberstalkers is worthy of further attention since it has implications for the safety of victims and how cyberstalking cases are dealt with.

It may be helpful to consider the role of feedback from the perspectives of cyberstalkers and victims. We can argue that cyberstalkers gain intrinsic and extrinsic feedback from their behaviour. *Intrinsic feedback* comes from actions taken and need not require interaction or communication with other people, including the victim. As an example, a cyberstalker may experience satisfaction once regular reports begin to arrive from a piece of spyware successfully planted on a victim's computer. *Extrinsic feedback* is normally derived from other people, most often from the reactions of the victim to the cyberstalker's acts. As an example, a response to an inflammatory message signifies that the victim received it and was sufficiently affected to reply. As noted earlier, even the lack of any reaction from a victim may be construed as a form of extrinsic feedback. The absence of a victim from a social media group, for instance, may indicate that she has left because of the harassment experienced.

Victim coping responses may also have an effect on the qualities of the feedback received by cyberstalkers. While there is very little research that looks at coping responses in relation to cyberstalking, the literature dealing with areas such as workplace aggression and bullying among young people may be of relevance. In discussing conflict-related behaviours, Davis and Capobianco suggest that victims may display passive or active responses to conflict. For them an *active response* is one where the victim takes "…some deliberate, overt action in response to the conflict or provocation" (Davis, Capobianco, & Kraus, 2016). The alternative is a *passive response*, which generally involves the victim deciding not to take any action (ibid).

Passive responses can involve ignoring or avoiding conflict situations, or sometimes even denying that a problem exists (Zapf & Gross, 2010). In relation to cyberstalking, Tokunaga and Aune (2015) say that "…victims may consider more passive forms of risk management, such as ignoring or avoiding the pursuit." By effectively submitting to harassment, passive victims are likely to suffer more harm than active ones. As an example, in a study of bullying among 2,805 Finnish undergraduate students, Sinkkonen, Puhakka, and Meriläinen (2014) found that those who responded passively experienced problems such as "…weakening of capacity, motivation and self-confidence, low spirits and even depression". Furthermore, in a study of workplace conflict, Dijkstra, Dreu, Evers, and Dierendonck (2009) concluded that their results "…suggest that passive conflict behaviour is unconditionally detrimental."

For cyberstalkers, passive and active responses are likely to produce different kinds of feedback. Passive responses may reinforce the cyberstalker's perception of having power over the victim, while active responses may be seen as a challenge to that power. Depending on the cyberstalker's personality, he might be enraged either by the lack of engagement from a passive victim, or from the perceived defiance shown by a more active one. What little research evidence exists appears to support the idea that victim responses may encourage or discourage online harassment. In a survey of "cybervictimisation" among young Americans, Hawdon et al. (2017) found that confrontational styles of conflict resolution place people at increased risk of victimisation, while tolerating hostile behaviour does not significantly increase the risk of being victimised.

The OVIAR model may also help to explain the time compression phenomenon that some writers have identified in relation to cybercrime and cyberstalking. Landry (2008) for example, discusses how technology helps to reduce or eliminate the distance between cybercriminals and their victims. He also explains how many tasks can now be accomplished quickly and more easily than before, including criminal acts. Landry's work expands upon (Bocij, 2003) argument that cyberstalking cases tend to unfold more quickly than offline stalking cases. This is partly due to the efficiency that technology adds to activities such as searching for information but is also related to the satisfaction that the cyberstalker obtains from victim feedback. In the context of the OVIAR model, if feedback received online is somehow less satisfying than real-world feedback, this may cause the cyberstalker to accelerate each cycle of harassment.

A greater understanding of how the feedback from victims affects a cyberstalker's behaviour is an essential step towards protecting victims and reducing harassment. In terms of the model presented here, it may also play a critical part in halting the cycle shown in the diagram.

The cycle shown may repeat many times before the harassment stops. In some cases, the harassment will end permanently, for instance if the cyberstalker is apprehended or moves on to another victim. In other cases, there may only be a respite before a new cycle of harassment begins. There can be many reasons for a break in the cycle of harassment perpetrated by stalkers and cyberstalkers (Krull & Shukyn, 2015; Snow, 2007). If the victim moves home, for instance, it may take time for the cyberstalker to locate her again. The cyberstalker's activities may also be temporarily halted if he is incarcerated for a time. A cyberstalker may also reappear from time to time to remind the victim that he is still there, or to see if his reappearance elicits the reactions he enjoyed before.

There are also a number of other decision points throughout the model where the cyberstalker must decide whether or not to continue his pursuit of the victim. In some cases, this may be an emotional decision made hastily and without careful thought. In others, the decision may be more considered and may take into account costs versus benefits.

It is recognised, however, that the decisions made by a cyberstalker are likely to be influenced by a number of factors such as his own personal characteristics (e.g. low self-control) or the characteristics of the situation. Piquero and Tibbetts (2002) discuss the notion of a *control balance framework* and how it may influence the decisions made by deviants by affecting how they assess the costs and benefits associated with their actions. Vito, Maahs, and Holmes (2007) go further and suggest that "…offenders are likely to be irrational regarding the threat of apprehension". In this way, for instance, a cyberstalker might choose to believe that the chances of being caught are very low and may go on to take risks that seem reckless to an outside observer.

Resolution occurs when the harassment ends or is reduced to a point where it no longer affects the everyday life of the victim. As suggested earlier, there may be many reasons why cyberstalking ends: the cyberstalker may move on to a new victim; he may lose track of the victim if she moves away or changes her online persona; or he may be identified and prosecuted.

It is suggested that a threshold of six months should be used to identify the end of an episode of harassment. This is because there is some evidence to suggest that most cyberstalking episodes end after

approximately six months (Al Mutawa, Bryce, Franqueira, & Marrington, 2016; Bocij, 2003; National White Collar Crime Center, 2015) a figure in keeping with the typical length of offline stalking cases (B. Fisher & Lab, 2010; Schwartz-Watts, 2006). However, it is recognised that setting any threshold may be problematic This is because some cases of cyberstalking may last for several years and there may be relatively long gaps between individual cyberstalking episodes. Victims may come to believe that the harassment has ended only to find that it restarts some time later. A number of writers have reported cyberstalking cases that have lasted for several years (e.g. (Al Mutawa et al., 2016; Tokunaga & Aune, 2015; Wallace, 2016)). For some victims of cyberstalking, this means that resolution may be temporary or permanent as there is no way of knowing if or when the harassment will resume, especially in cases where the identity of the cyberstalker is not known.

Despite the difficulties presented by using a six-month cut-off point, it is argued that some way of determining when or if a period of harassment is likely to have ended is necessary, even if for no other reason than to hearten victims. Using a threshold may also provide a common means of measurement. This is likely to provide a way of making meaningful comparisons between studies.

As mentioned earlier, an episode of cyberstalking may end for a variety of reasons, many of which may be outside of the control of the cyberstalker or the victim. Cases may end because of the actions of one or more other actors, including law enforcement or the victim's spouse, colleagues, friends or relatives. Thus, resolution may occur without any action on the victim's part and she may not even know that others have interceded.

3. Using the Model

One of the ways in which the OVIAR model can aid efforts at reducing cyberstalking is by identifying points at which a cyberstalker's activities can be disrupted or possibly prevented altogether. In this section of the discussion, a focus is placed on the *Initiation*, *Intelligence* and *Feedback & Evaluation* stages since it is felt that these best illustrate the model's practical application as means of mitigating cyberstalking incidents.

In the *Initiation* stage, an emphasis should be placed on avoiding becoming the focus of a potential cyberstalker's attention. Benjamin Franklin's view that "An ounce of prevention is worth a pound of cure" holds true here; preventing a potential cyberstalker from pursuing the victim in the first place is easier than attempting to intervene after the cycle discussed here has become a routine behaviour. This may involve relatively simple preventative measures, such as those suggested by online safety organisations. Many organisations[i], for example, advise Internet users to choose gender-neutral e-mail addresses and user names. While many of these measures are quick and inexpensive, many Internet users fail to use them, suggesting a need for greater education about online safety. Additional protection can be gained if users also consider their online behaviour and make efforts to reduce or eliminate things that may be seen as provocative by a potential cyberstalker. Again, this suggests a need for greater education about "netiquette", informal rules for acceptable online behaviour. There is also some evidence to suggest that understanding more about how to behave online can reduce the likelihood of someone starting to harass others. Several studies of young people have shown that a good understanding of netiquette can reduce bullying and cyberbullying. As an example, a survey of 1,200 young people aged 12 to 15 by Park, Na, and Kim (2014) found that those given a good understanding of netiquette were less likely to become cyberbullies. A study of more than 4,000 elementary, secondary and high school students by Kumazaki, Suzuki, Katsura, Sakamoto, and Kashibuchi (2011) found that a good understanding of netiquette significantly decreased school bullying. While the authors did not find that cyberbullying could be reduced, they noted that this may have been due to methodological issues and concluded that "…education in good netiquette is… necessary to prevent cyber-bullying" (Kumazaki et al., 2011).

It is worth noting that there is some debate about whether Internet users should be forced to change their behaviour in order to avoid the attention of a potential harasser. This dialogue is ongoing and there appear to be no simple answers capable of satisfying each side of the debate. While further discussion is beyond the scope of this paper, it is acknowledged that this is an important area worthy of further consideration by academics and other stakeholders. Whichever view ultimately gains dominance, there will be significant implications for the way in which we view and respond to online harassment. Given that access to the Internet is now seen as a human right by many countries (Howell & West, 2016) this paper adopts the view that Internet users should enjoy the same rights online as they do offline. Put simply, it is felt that the principle of free speech applies to the online world as well as the physical world, so asking the victims to stop using certain services or remain offline for a time is unacceptable. Returning to the *Initiation* stage of the proposed model, once the cyberstalker decides to act against the victim he enters the first iteration of the intelligence-planning-action-feedback cycle. The first part of this cycle, the *Intelligence* stage, is important because an intervention occurring here can halt the rest of the cycle. If the cycle is disrupted during the first iteration, it may prevent the cyberstalking altogether. If the intervention occurs in a later iteration, the disruption might influence the *Feedback & Evaluation* stage, causing the cyberstalker to lose interest in the victim more quickly than he might otherwise. It is known that cybercriminals often profile their victims, drawing upon publicly accessible information such as social networking profiles (Arief & Adzmi, 2015; Atta-Asamoah, 2009). Cyberstalkers also create profiles, often connecting information drawn from different sources in order to create extraordinarily

detailed dossiers documenting their victims' lives. Bocij (2004) for instance, describes an incident where a profile of a young woman was created using freely available tools. The profile was so detailed that it even contained the name of the woman's dog. Research by Welsh and Lavoie (2012) suggests that as people spend more time using social media, they become accustomed to disclosing personal information about themselves. In turn, this increases the risk of them becoming victims of cyberstalking.

One way of disrupting the intelligence-planning-action-feedback cycle is by controlling what information about the victim is available online. As already mentioned, limiting the information available to a harasser during the *Intelligence* stage will reduce the number of actions available to him, making it more difficult to pursue the victim. In order to make it difficult for a cyberstalker to develop a profile of the victim, two main approaches might be used. The first involves making sure that the different aspects of a person's online life are disconnected from one another. This makes it harder to locate, verify and collate information about the victim. A good example of this might be the adoption of different user names for each online service used. Unless the harasser knows each user name, it will be difficult for him to find the victim's online personas. Other measures, such as using different e-mail addresses for online accounts, can complicate things further for the harasser.

The second approach involves misdirecting the harasser by changing or removing the information shown in online profiles and directories. Omitting or entering the wrong gender, for instance, will often mean that the victim's information will not appear in the typical searches carried out by the harasser.

The *Feedback & Evaluation* stage also provides opportunities to curtail a cyberstalker's activities. As mentioned earlier, starving the cyberstalker of feedback on his actions may cause him to lose interest in the victim, though there is also the risk that the harassment might escalate. Also mentioned earlier is that a further problem lies in determining what may constitute meaningful feedback to the cyberstalker. It might be argued that any reaction might be interpreted in a way that encourages further harassment and that even silence might be seen as evidence that the victim is in fear. Despite the risk of escalation and a lack of relevant research evidence, it is felt that displaying no reaction to the harassment is likely to be the best course of action in the majority of cases. This is supported in part by studies of offline stalking which have shown that actions involving communication with stalkers, such as attempting to reason with them or even taking legal action, do little to discourage them and may even make matters worse (Brewster, 2001; Sheridan, Davies, & Boon, 2001). As discussed earlier, even when the *Resolution* stage is reached, there is a risk that the harassment may begin again some time later. The same measures that one might take measures to avoid becoming a victim in the first place are likely to reduce the risk of revictimisation. Using multiple user names, for instance, may prevent the cyberstalker from locating the victim.

4. Conclusion

The OVIAR model provides a representation of the dynamics and lifecycle of online victimisation, such as cyberstalking. The model suggests that cyberstalking is iterative in nature meaning that a cyberstalking episode may involve a number of cycles, each of which represents an individual act of harassment. In each cycle, the cyberstalker will need to gather information, plan, take action against the victim in some way and then obtain feedback on his actions. If the model's depiction is accurate, it may suggest that the victim's situation can be alleviated by disrupting the cycle. In particular, it is possible to identify a number of decision points where an appropriate intervention may discourage the cyberstalker from committing further acts of harassment. As an example, the actions of a cyberstalker are often dictated by the information he has available concerning the victim. If he is denied this information, his choices about how he might pursue the victim become restricted. Cyberstalkers may also be discouraged by depriving them of the feedback received from victims. However, further research is needed to assess the risk that a victim's silence may result in escalation.

The OVIAR model is offered as a framework for further discussion and research. It is intended that others build upon its strengths and find ways to mitigate any weaknesses. The model may also form the basis for the development of more practical tools that can be used to manage cases of online victimisation.

List of Abbreviations

OVIAR - Online Victimisation Intervention & Reduction (Model)

References

Al Mutawa, N., Bryce, J., Franqueira, V. N. L., & Marrington, A. (2016). Forensic investigation of cyberstalking cases using behavioural evidence analysis. *Digital Investigation*, *16*(S), S96-S103. Available at: https://doi.org/10.1016/j.diin.2016.01.012.

Arief, B., & Adzmi, M. A. B. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 2--defenders and victims. *IEEE Security & Privacy*, *13*(2), 84–88. Available at: https://doi.org/10.1109/MSP.2015.44.

Atta-Asamoah, A. (2009). Understanding the West African cyber crime process. *African Security Review*, *18*(4), 105–114. Available at: https://doi.org/10.1080/10246029.2009.9627562.

Bocij, P. (2003). Victims of cyberstalking: An exploratory study of harassment perpetrated via the internet. *First Monday*, *8*(10). Available at: https://doi.org/10.5210/fm.v8i10.1086.

Bocij, P. (2004). *Cyberstalking: Harassment in the internet age and how to protect your family*. Westport, Conn., London: Praeger Publishers.

Bocij, P. (2005). Reactive stalking: A new perspective on victimisation. *British Journal of Forensic Practice*, *7*(1), 23–34.
Bocij, P., Greasley, A., & Hickie, S. (2015). *Business information systems: Technology, development and management*: Pearson Education.
Bocij, P., & McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*, *139*, 31–38.
Bocij, P., & McFarlane, L. (2003). Seven fallacies about cyberstalking. *Prison Service Journal*, *149*, 37–42.
Brewster, M. (2001). Legal help–seeking experiences of former intimate–stalking victims. *Criminal Justice Policy Review*, *12*(2), 91–112.
Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394–402. Available at: https://doi.org/10.1016/j.chb.2017.03.061.
Davis, M. H., Capobianco, S., & Kraus, L. A. (2016). Measuring conflict-related behaviors: Reliability and validity evidence regarding the conflict dynamics profile. *Educational and Psychological Measurement*, *64*(4), 707–731. Available at: https://doi.org/10.1177/0013164404263878.
Daynes, K. (2012). Is there a psychopath in your inbox? The Telegraph. Retrieved from http://www.telegraph.co.uk/lifestyle/9064008/Is-there-a-psychopath-in-your-inbox.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. Available at: https://doi.org/10.1108/JACPR-06-2016-0234.
Dempsey, J. S. (2010). *Introduction to private security*. Boston, USA: Cengage Learning.
Dijkstra, M. T. M., Dreu, C. K. W., Evers, D. A., & Dierendonck, V. D. (2009). Passive responses to interpersonal conflict at work amplify employee strain. *European Journal of Work and Organizational Psychology*, *18*(4), 405–423. Available at: https://doi.org/10.1080/13594320802510880.
Donovan, F., & Bernier, K. (2009). *Cyber crime fighters: Tales from the trenches*. Indianapolis, Ind: Que.
Dressing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior and Social Networking*, *17*(2), 61–67. Available at: https://doi.org/10.1089/cyber.2012.0231.
Fisher, B., & Lab, S. (2010). *Encyclopedia of victimology and crime prevention*. California, USA: Sage Publications, Inc.
Fisher, B. S., & Sloan, J. J. (2013). *Campus crime: Legal, social, and policy perspectives* (3rd ed.). Springfield, Ill., USA: Charles C. Thomas, Publisher.
Glass, D. (2006). *Stalking the stalker: Fighting back with high-tech gadgets and low-tech know-how*: Diane Glass.
Haider, D., & Jaishankar, K. (2009). Cyber socializing and victimization of women. *Temida*, *12*(3), 5–26. Available at: https://doi.org/10.2298/TEM0903005H.
Hawdon, J., Costello, M., Ratliff, T., Hall, L., & Middleton, J. (2017). Conflict management styles and cybervictimization: Extending routine activity theory. *Sociological Spectrum*, *37*(4), 250–266. Available at: https://doi.org/10.1080/02732173.2017.1334608.
Hazelwood, R. R., & Burgess, A. W. (2009). *Practical aspects of rape investigation: A multidisciplinary approach. CRC series in practical aspects of criminal and forensic investigations* (4th ed.). Boca Raton: CRC Press.
Hazelwoode, S., & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. *International Journal of Cyber Criminology*, *7*(2), 155–168.
Howell, C., & West, D. (2016). *The internet as a human right*. Brookings. Washington DC, United States: Brookings Institution.
Jaishankar, K. (2011). *Cyber criminology: Exploring Internet crimes and criminal behavior*. Boca Raton, FL: CRC Press.
King-Ries, A. (2011). Teens, technology, and cyberstalking: The domestic violence wave of the future? *Texas Journal of Women and the Law*, *20*(2), 131–164.
Kirwan, G. (2011). *The psychology of cyber crime: Concepts and principles*. Hershey, PA, USA: Information Science Reference.
Krull, A. K., & Shukyn, M. (2015). GED RLA for dummies: Wiley. Retrieved from https://books.google.co.uk/books?id=kQKKCgAAQBAJ.
Kumazaki, A., Suzuki, K., Katsura, R., Sakamoto, A., & Kashibuchi, M. (2011). The effects of netiquette and ICT skills on school-bullying and cyber-bullying: The two-wave panel study of Japanese elementary, secondary, and high school students. *Procedia - Social and Behavioral Sciences*, *29*, 735–741. Available at: https://doi.org/10.1016/j.sbspro.2011.11.299.
Landry, J. (2008). Time and space compression in criminology. *Professional Issues in Criminal Justice*, *3*(2), 87–96.
Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. Available at: https://doi.org/10.1080/01639625.2015.1012409.
Lipsey, M., & Landenberger. (2006). Cognitive-behavioral intervention. In Welsh, B.C. and Farrington, D.P. (Eds.), (2006) Preventing Crime: What Works for Children, Offenders, Victims and Places (pp. 57-72). Netherlands: Springer.
Magnet, S., & Gates, K. (2013). *The new media of surveillance*. Hoboken: Taylor and Francis.
Miller, M. (2008). *Is it safe? Protecting your computer, your business, and yourself online*. Indianapolis, Ind: Que.
Mullen, P. E., Pathé, M., & Purcell, R. (2008). *Stalkers and their victims* (2nd ed.): Cambridge University Press.
Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2016). Do routine activities help predict young adults' online harassment: A multi-nation study. *Criminology & Criminal Justice*, *17*(4), 418–432. Available at: https://doi.org/10.1177/1748895816679866.
National Centre for Cyberstalking Research. (2015). *A practical guide to coping with cyberstalking*. Luton: Andrews UK.
National White Collar Crime Center. (2015). Cyberstalking. Retrieved from http://www.nw3c.org/docs/research/cyberstalking.pdf?sfvrsn=10.
Park, S., Na, E. Y., & Kim, E. M. (2014). The relationship between online activities, netiquette and cyberbullying. *Children and Youth Services Review*, *42*, 74–81. Available at: https://doi.org/10.1016/j.childyouth.2014.04.002.

Pathé, M. (2002). *Surviving stalking*. Cambridge: Cambridge University Press.
Pinals, D. A. (2007). *Stalking: Psychiatric perspectives and practical approaches*. New York, Oxford: Oxford University Press.
Piquero, A. R., & Tibbetts, S. G. (2002). *Rational choice and criminal behavior: Recent research and future challenges Current issues in criminal justice*. New York, London: Routledge.
Pyrooz, D. C., Decker, S. H., & Moule, R. K. (2013). Criminal and routine activities in online settings: Gangs, Offenders, and the internet. *Justice Quarterly, 32*(3), 471–499. Available at: https://doi.org/10.1080/07418825.2013.778326.
Radford, K. J. (2013). *Individual and small group decisions*. New York: Springer New York.
Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behavior, 33*(1), 1–25. Available at: https://doi.org/10.1080/01639625.2010.538364.
Schwartz-Watts, D. (2006). Commentary: Stalking risk profile. *Journal of the American Academy of Psychiatry Law, 34*(4), 455–457.
Sheridan, L., Davies, G., & Boon, J. (2001). The course and nature of stalking: A victim perspective. *The Howard Journal, 40*(3), 215–234.
Sinkkonen, H. M., Puhakka, H., & Meriläinen, M. (2014). Bullying at a university: Students' experiences of bullying. *Studies in Higher Education, 39*(1), 153–165. Available at: https://doi.org/10.1080/03075079.2011.649726.
Snow, R. (2007). *Stopping a stalker: A cop's guide to making the system work for you*. New York, USA: The Perseus Books Group.
Tokunaga, R. S., & Aune, K. S. (2015). Cyber-defense: A taxonomy of tactics for managing cyberstalking. *Journal of Interpersonal Violence, 32*(10), 1451–1475. Available at: https://doi.org/10.1177/0886260515589564.
Vito, G. F., Maahs, J. R., & Holmes, R. M. (2007). *Criminology: Theory, research, and policy. Criminal justice illuminated* (2nd ed.). Sudbury, Mass and London: Jones and Bartlett.
Wallace, P. M. (2016). *The psychology of the internet* (2nd ed.). New York: Cambridge University Press.
Wang, W. (2006). *Steal this computer book 4.0: What they won't tell you about the internet*. San Francisco, Calif: No Starch.
Welsh, A., & Lavoie, J. A. A. (2012). Risky ebusiness: An examination of risk-taking, online disclosiveness, and cyberstalking victimization. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6*(1). Available at: https://doi.org/10.5817/CP2012-1-4.
Zapf, D., & Gross, C. (2010). Conflict escalation and coping with workplace bullying: A replication and extension. *European Journal of Work and Organizational Psychology, 10*(4), 497–522. Available at: https://doi.org/10.1080/13594320143000834.

[i] Examples include WHOA (http://www.haltabuse.org/resources/online.shtml), AOL (https://help.aol.co.uk/articles/top-10-tips-for-online-safety) and APC (https://www.apc.org/en/pubs/issue/how-avoid-becoming-cyberstalking-victim)