IJWR

Criminological Study of Personality-Based Crimes in Cyberspace; from Typology to Policy Strategies

Ehsan Salimi[a*], Sepideh Bouzari[b], Parviz Dehghani[c]

Assistant Professor, dept. of Humanities, University of Maragheh, Maragheh; Iran. e.salimi@maragheh.ac.ir [a]; bozari.s@maragheh.ac.ir [b], p.dehghani1351@maragheh.ac.ir [c]

ABSTRACT

Harassment-based crimes targeting the spiritual integrity of victims are among the most numerous and varied offenses in cyberspace, ,which can be categorized under the general title of harassment in cyberspace. According to the unique properties and meta-variables of information and communication technology, the rate of harassment crime in cyberspace is more than that of real space. This study, a descriptive-analytical meta-analysis, aims to critically examine personality-based crimes and harassment in cyberspace. It seeks to identify the types of crimes, the characteristics of the victims, and the criminal profiles of the offenders. Findings reveal that these crimes are predominantly perpetrated by young men with diverse motivations, particularly of a sexual nature, targeting teenage girls. Based on these findings, it is recommended that legislators adopt a differential and aggravated approach to criminalize harassment against women and children. Additionally, addressing the role and needs of victims in crime responses is crucial. Furthermore, identifying and criminalizing emerging personality-based behaviors, balancing crime platform filtering, adopting participatory criminal policies involving non-governmental organizations, empowering users with preventive oversight and technical measures, and enhancing media literacy and cultural norm-setting are essential strategies for combating personality-based crimes.

Keywords*— Cyber Harassment, Restorative Justice, Criminal Profiling, Participatory Criminal Policy, Filtering, Cyber Criminology.*

1. Introduction

Criminology has encountered a new world at the beginning of the 21st century that has made it easy to speak about the globalization of crimes. The current criminology and criminal deficiencies about cybercrimes have provided committing the crime for common citizenry in cyberspace in addition to the criminals. Considering some specific features of cyberspace, aberrations, and crimes have caused some people to think of the internet as a storehouse of weapons for social inhumanity, and these cases are growing increasingly and annoyingly [1]. Correspondingly, recognizing these cybercrimes properly is highly necessary to fight these crimes. In line with the restorative justice as a relatively new paradigm and based on the subject of victimization, cybercrimes can be categorized into two main types: data crimes and personality crimes. "Spiritual personality" is the target in personality-driven crimes. Thus, instances of personality-driven crimes can be defined as various forms of harassment that occur in computer or telecommunication systems against an individual. In contrast, in data crimes, the subject of the crime is the data stored in repositories or telecommunication systems. Personality crimes occur in an interactive process and human communication. In contrast, data crimes may occur in solitude by criminal without any direct interaction with others. The role of the victim in prevention and occurrence of a crime is active and influential. In data crimes, the criminal equipment and tools, as well as those used for prevention, play a fundamental role in both preventing and committing the crime. The costs of personality crimes are often extensive and difficult to estimate. Even victims of these crimes may carry the psychological effects of victimization for years after the incident, extending

http://dx.doi.org/10.22133/ijwr.2024.446635.1206

Citation E. Salimi, S. Bouzari, P. Dehghani, "Criminological Study of Personality-Based Crimes in Cyberspace; from Typology to Policy Strategies", *International Journal of Web Research*, vol.7, no.1,pp.49-60, 2024, doi: http://dx.doi.org /10.22133/ijwr.2024.446635.1206.

**Coressponding Author*

Article History: Received: 2 November 2023 ; Revised: 24 December 2023; Accepted: 7 January 2024.

Copyright © 2022 University of Science and Culture. Published by University of Science and Culture. This work is licensed under a Creative Commons Attribution-Noncommercial 4.0 International license(https://creativecommons.org/licenses/by-nc/4.0/). Noncommercial uses of the work are permitted, provided the original work is properly cited.

beyond the cyber space into their everyday lives. However, in data crimes, although the costs of victimization can sometimes be extensive, they are estimable, and the period of victimization can be identified (Figure 1).

The significant outcome of this innovative categorization lies in its ability to differentiate policy-making for personality crimes, considering the prominent role of human agency. When the personality is the target of victimization, empowering them can prevent crime from occurring in the first place. In brief, because personality crimes directly target an individual, policy strategies for prevention and criminal measures differ significantly from cases where the direct subject is computer data. This study aims to identify effective policy strategies for addressing personality crimes in cyberspace. To achieve these strategies, a study of the criminology of personality crimes has been placed on the agenda. Identifying comprehensive aspects of various facets of these crimes is a prerequisite for effective, proportionate, and responsive strategies aligned with the causes and factors of victimization. Thus, this article begins with the conceptualization of personality criminal behaviors and then proceeds to identify the types and platforms where these crimes occur. Following that, the article focuses on understanding the criminal profiles of criminals and victimology of these crimes. Finally, it outlines effective strategies and policies to combat these crimes, taking into account the dynamics of the crime, the criminal, and the victim.

2. Literature Review

Significant studies have been conducted on personality-driven cybercrimes. For instance, in 2024, Rosemary et al. published a paper titled "The Relationship between Anonymity and Cyber Sexual Harassment by Twitter Users: A Cross-Sectional Study." They have concluded that there is a relationship between anonymity and Twitter users' inclination to engage in cyber sexual harassment. In such a way that the less anonymity there is, the lower the inclination towards cyber sexual harassment tends to be [2]. Walters et al., in 2020 published another article titled "Assessing the Relationship between Cyber and Traditional Forms of Bullying and Sexual Harassment: Stepping Stones or Displacement?" Walters focused on the relationship between cyber bullying and face-to-face bullying, testing two hypotheses. The first hypothesis was that young criminals of cyber bullying would also engage in face-to-face bullying. The second hypothesis was that cyber bullying offenders seek revenge for previous harassment in

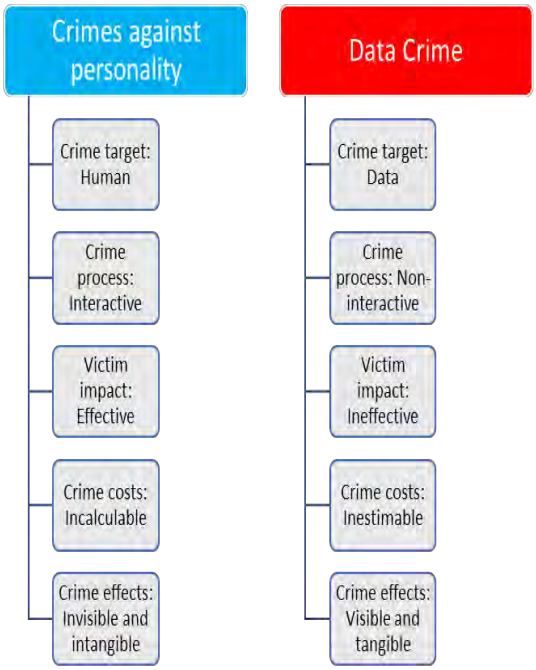

Figure. 1. Comparison of data-based crimes and personality-based crimes

real life, which researchers ultimately found to reject the first hypothesis and support the second one as being closer to the truth [3].

Tracy Vaillancourt, Robert Faris, and Faye Mishna (2017) [4] and McDougall, Vaillancourt (2015) [5] found that cyber bullying is associated with significant short- and long-term mental and physical health issues. However, it is the cyber bully/victims that appear to be the most high risk group reporting higher levels of psychological and health issues including post-traumatic stress, mental health impairment, anxiety, self-esteem, academic performance, and depression [6]. Victims of cyber bullying report an array of psychopathologicalsymptoms, including internalizing problems such as feelings of loneliness, depression and lack of self-esteem [7]. Moreover, it has been related to social anxiety and isolation as well as to externalizing problems, illicit drug use and conduct problems [8].

Despite significant studies conducted and the rich scholarly literature on the subject, the dynamic nature of the cyber space and the emergence of new crimes necessitate the undertaking of the present study. Furthermore, this article provides an innovative approach by addressing corresponding and proportionate policy aspects aligned with the findings of criminological research.

3. Conceptualizing Personality-Driven Harassing Behaviors in Virtual Spaces

The cyber harassment prevalence and bullying varies depending on whether a broad or narrow definition is applied [7]. Creating harassment in cyberspace is a wide concept and example. This means that some of these disruptive-kind behaviors have not been termed with a specific name despite having the harassment feature in their behavioral nature. Unfortunately, young users of the internet cannot participate in online activities without encountering harassment of an uninvited relationship by other internet users [1]. These undesirable behaviors are comparable with their parallels in the real space to some extent; however, they have their specific kinds and tools as well. The duplication of the activities and the relationships of people, and accordingly, the duplication of criminality causes committing traditional crimes in the environments or by cyberspaces on one hand. On the other hand, crime commitment has had special crimes in this field [9]. In the following, the conceptology of cyber harassment is compared with classic harassment, and after that, the tools of crime are discussed.

The concept of crime can be analyzed in two classic and cyber categories, considering the twofold space of life in these two classic spaces (real world) and cyberspace categories [10]. Cyber harassment almost comes from classic harassment, in which the criminal uses modern technology to commit the crime. The classic crimes, in which information technology is used are known as cyber-based crimes [11]. The obtrusive criminals, including classic and online ones, use the behaviors and tactics to create nuisance and sometimes threaten and frighten the victim. The other similarity that exists between classic and online harassment is that the parties of the crime most probably have had a real or unreal friendly relationship in the past. In this regard, cyber harassment probably selects its victims randomly [11]. Some types of cyber harassment have traditional roots, meaning that these harassments happen face to face in the real world. Thereafter, these harassments occur via electronic instruments by entering into cyberspace and removing the presence feature [12].

Another similarity between various types of cyber and classic harassment is their shared risk factors and backgrounds, as some researchers believe that certain risk factors such as low peer support, anger, and patriarchy [13, 14]. As an example, one of the harassments that occur without using cyberspace is bullying in school that happens in the school environment. The bullying in school was transferred to cyberspace after the presence of cyberspace in the existent environments, and it changed to cyberbullying [15]. One of the apparent differences between classic and cyber harassment is the geographical distance between the criminal and the victim in classic harassment. In terms of classic harassment, the criminal and victim often have the same place of life and work; nevertheless, the cyber intruder can harass their victims in their home on the corner of a street, in an internet café in another city, and even in another country. In other words, cyber harassment is different from classic harassment in terms of method, nature, and type of crime that require new studies, regarding criminology, penology, and criminal justice. By referring to the differences and similarities between classic and online harassment and the concept that was described about cyber harassment, a definition is achieved for cyber harassment. That is "cyber harassment as a crime against the spiritual personality is a general title for each deliberate and scientific action against reputation, credit, and calmness of real person, using the information and communication technology".

4. Platforms of personality-driven crimes

Offenses against the person or personality-driven cybercrimes can be defined as a crime committed by introducing oneself. It means that to commit this crime, the use of a specific tool, which is the internet and cyberspace, is necessary. Although the possibility of this crime occurring exists in all cyberspaces, certain places and tools will provide a more suitable platform for cyber harassment (Figure 2).

Figure. 2. Crime Platforms

4.1. Social Networks

Although the websites of social networks have opened a new window towards socialization, it is the beginning of various crimes against people, especially, women in cyberspace. The current legal and psychological research about the adventurous function of cyber and the effects after that has proved that social networks pose more risks than chatrooms on the internet [16]. Most types of cyber harassment that were mentioned above occur in these social networks. Social network users can publish baseless and cruel rumors about others who are present on a social website that might be observed by hundreds of online friends. Social networks can create many examples of online harassment, including hate speech in cyberspace, cyberbullying, and changed pictures.

These social networks can easily attract teenage girls and women since these victims believe that the risk of unknown sex hunters or the issues of privacy are low in these networks. However, most of them have neglected that their identity can be abused with stalking intent [16]. Correspondingly, they are abused for offline sexual assault, harassment, identity theft, cyber sexual harassment, online cheating, and potential victimization.

4.2. Email

Some older research studies indicate that cyber harassers primarily use email for harassing, intimidating, and threatening their victims [17]. Although doubts can arise after the emergence of social networks, email remains one of the most common tools used for cyber intimidation. The study findings report that cyber intruders often use other electronic communicative tools, mostly Email to harass and threaten the victims, and this is the most common tool that is used for cyber frightening. Email permits the criminal to frequently send hurtful, disgusting, and nasty messages, such as pictures, movies, and voice with high speed and comfort. In most cases, cyber intruders use email addresses and other personal information to subscribe to or buy books, magazines, or other online services without the victim's knowledge and consent. Unfortunately, some websites permit users to use free emails with the least personal information. Although these websites ask the users to list their identity information, they rarely confirm the presented documents; thus, the efforts of law enforcement will be more useless. Moreover, some of the email servers delete the identity information intentionally by achieving a small amount, and this action makes it more difficult for law enforcement to track emails. A smart cyber intruder uses computer applications alternately that are specific for frequently sending emails to more audiences with regular or random time intervals. Besides, such criminal most probably uses anonymous emails which makes it impossible to track the sending point by the law enforcement [18]. Inventing spy software has enabled criminals to buy applications with low cost which have been designed to inform the criminal about getting online by the victim [17].

4.3. Entertainment Websites

Chatrooms and discussion-based forums are usually the platforms by which online users express and explain their perspectives about one or several subjects. Discussion forums can be a place for cyber stalkers to harass others and access their personal information, including name, address, phone number, email address, and confidential information [17]. Some of the websites, such as http://www.myspace.com permit the users to exchange sensitive and personal information about each other. The issue that such users are not aware of is that the information is available on the website, and the public can access it as well. As an example, some of the websites permit users to send half-naked pictures of women, send obscene remarks about women, and share pornographic images with all the members. Moreover, some websites encourage the members to use violence and immorality. A website entitled "Release your rage" encourages the users to release their failure and rage on a specific person who might not be from the members or to use insulting words.

4.4. Virtual Business Platforms

Digital platforms have become a new platform for various interactions among individuals [19]. Online business platforms are software infrastructures that allow economic actors and traders to analyze markets and manage their transactions. In fact, trading platforms act as intermediaries between traders and brokers. The Information Technology & Innovation Foundation defines digital platforms as online businesses that facilitate commercial transactions between at least two groups, typically one being a supplier and the other a consumer. Amazon and eBay are examples of e-commerce platforms, facilitating transactions for buying and selling goods. Although these platforms are relatively new, the research literature in the field of platform criminology, especially offenses centered around harassment, has not fully matured. Reliable statistics regarding the extent and nature of criminal activities on these platforms are not yet available. However, activities on platforms and observations within platform spaces indicate that certain offenders have migrated their interactive and personality-driven crimes to these

environments, engaging in a spectrum of criminal behaviors in these spaces.

5. Typology of Personality-Driven Offenses in Cyberspace

As a result, personality-driven cyber offenses are said to have become pandemic or widespread [20]. In general, personality-driven offenses are a broad term for crimes such as cyber gossip, cyberstalking, morphing or impersonation, hacking, cyber harassment (in a specific sense), blocking a user and banning them from expressing their views, cyberbullying, defamation, identity theft, deception, and cyber slander, among others. In the following, brief explanations of the main types of cyber harassment, which are more prevalent and prominent in cyberspace, will be provided:

- **Cyber roorback:** refers to spreading humiliating or derogatory rumors about a victim in chat rooms, news groups, or online bulletin boards. One of the most common forms of cyber defamation involves sending false sexual innuendos about the victim [17].
- **Cyberstalking:** Cyberstalking refers to a situation in which a user is secretly followed in all the groups that she/he has joined. Moreover, the friends of this user are continuously monitored to see the posts, personal writings, and online activities of that user [21].
- **Simulating and imitating:** In this type of criminality, the criminals create a simulated or fake profile of the victim by stealing the user's personal information. Thereafter, the simulated profiles ask the user's friends to become friends with them. Thus, in addition to using the information of the original member for nefarious goals, in this case, one beyond step is taken in victimization by creating a gap in the privacy of other users. Today, most users in social networks, such as Facebook, My Space, and Orkut are unfortunately women and mostly experience these issues [22].
- **Morphing:** In this case, the pictures of the social network users are taken from their personal albums and are used for the purposes of obscenity and defamation of the users. This happens by using a section of the picture, such as head and face which are the representative of the user, and the rest of the picture can be changed and manipulated. Morphing or distortion manifests differently: sometimes, transformation in another content is like obscenity. Besides, transformation causes desecration which is recognized here with the custom of crime [23]. Further, the obtrusive person might send obscene messages to the victim's page.
- **Cyberbullying:** In this method, the obtrusive person might continuously apply humiliation and bullying for the victims on the social networks on their page and in the groups and the meeting places that the victims attend. This type of crime might be permanently sending text messages to the original user's page or other platforms.
- **Sexual harassment:** This type of crime includes demanding sexual requests on the victim, without obtaining his/her consent, and this is one of the most social harms in all countries, including the under-developed, developed, and at all social levels. Sexual harassment in cyberspace occurs more than its classic one due to the features of anonymity, the wide range of users, and the absence of necessary deterrence [15].
- **Insult and ridicule:** Insult and ridicule are significant examples of cyber harassment. These two harassments spread in cyberspace rapidly due to some features, such as entertaining this subject. This issue highlights the annoying aspect of ridicule and insult in cyberspace [15].
- **Disclosure of privacy:** Publishing other private information such as text, audio, image or other secrets includes the behavior of disclosing and making available another's privacy more than all spaces in social networks. Because in these networks, often in groups or channels, a collection of familiar people whose private aspects of their lives are important to each other have gathered.
- **Unnecessary blocking:** Cases where a user blocks another person's social network or business platform unnecessarily. This type of crime has spread in social networks and recently in business platforms.. Harassment by competitors: Harassment that is often common in business platforms and is often done by a competitor's colleague or broker, or the harasser advertises his product/service in the chat. To some extent, such harassment is done on social networks and often on business platforms.
- **Impersonation:** Cases in which an intruder has given another person's number instead of his own in a trading platform. Often in virtual platforms, this type of crime is common because people exchange numbers in order to communicate more in this environment.

- **Dumping of information:** Cases where the person requested information such as address, phone number and card number and in this way sought to dump information. Sometimes, in business platforms, the harasser introduces himself as an expert or the operator of the platform and asks for information.
- **Begging:** Instances where the harasser requests financial assistance or mobile phone credit on a social network or business platform. This type of offending is becoming increasingly common on virtual platforms.

6. Criminal Profiles of Cyber Harassers

6.1. Offender Personality Types

Bocij and McFarlane (2005) conducted one of the most comprehensive studies on cyber harassers and victims of this type of harassment. According to the findings of this research, cyber harassers are classified into four distinct groups:

- **Vindictive cyber stalker:** Vindictive cyber stalkers have an evil-mind personality and harass and threaten their victims more than the other three groups. These criminals probably use numerous vindictive tactics to continuously hurt the victims via sending many spam, emails, and thieving their identity.
- **Composed cyber stalker:** Composed cyber stalkers determine their victims composedly and without any fuss. The primary purpose of this group is to harass, confuse, and create permanent anxiety for the victim by applying threatening behaviors.
- **Intimate cyber stalker:** The primary purpose of the intimate cyber stalker is to make a relationship with a previous intention based on fascination or intellectual complexity. This group acts differently from other groups due to having a relationship with the victim in the past.
- **Collective cyber stalker:** As the name reveals, collective cyber stalkers are formed of two or several people who pursue one victim, and this group has extraordinary computer skills compared to other groups.
- **Hedonist cyber harasser:** This type of offender often behaves like a hunter in the virtual space, without prior connection to their victims and often without premeditation. They commit a crime if they find a target with no obstacles. Their crimes are typically sexual in nature, and they exhibit an introverted and solitary personality.
- **Opponent Cyber harasser:** This category of harassers, primarily active on business platforms, target acquaintances, friends, or colleagues engaged in similar activities or competition. They are often individuals who exert minimal effort and attempt to compensate for their perceived distance or envy towards others by undermining them.

Regarding what was mentioned, it can be claimed that in most cases, despite other criminals, the purpose of the cyber stalker is not the financial intention, vindictiveness, honorable motives, and such cases. Accordingly, a high percentage of online users enter this space for entertainment and accidentally commit cybercrimes due to the convenience of committing crimes and being unknown and faceless (Figure 3).

6.2. Age of Criminals

There is a significant difference between the usage of social networks by various generations and their motives for joining cyberspace. The current generation is called Internet generation or network generation. The investigated studies report that most of these users are 16-24-year-old youths in all countries, in which the age of online users has been estimated. Cyberbullying is one part of cyber harassment that is different from other harassment due to the traditional root that it has. This type of harassment often occurs among adolescent age groups (students), and a low level of violence is experienced here. Although there is no accurate

Figure. 3. Criminal personality type

statistic, probably, most cyber stalkers are located in the range of 16-24 years old, regarding what has been mentioned about the personality features of these stalkers.

6.3. Gener

The available statistic reports that men use the internet and online space more than women in various countries. In addition to the fact that the number of men is more than women as online users, most of the cyber stalkers are men. Moreover, studies have highlighted that females have more participation in indirect forms of harassment, such as "gossip". This issue of why women have more tendency to participate in such criminal behaviors is highly influential. It has been claimed that first, females have an innate tendency to take part in "indirect types" of frightening that guarantee the methods of exchanging gossip, fault-fighting, and spreading rumors [24]. Second, females generally are not able to confront face to face [25]. Accordingly, women desire to send rumors online to harass others rather than to harass victims directly.

In most cases, the stalker men attack the victim for sexual purposes (morphing and using the victim's picture for pornographic and cyberstalking intentions) and non-sexual purposes (stalking and bullying). However, the stalker women victimize other women due to differences in opinion, disgust, and vengeance, and such attacks might not be naturally sexual.

7. Victimology of Cyber Harassment

Everyone could be the victim of cyberstalking crime; nevertheless, some specific population groups are exposed to the risk more than others, including women, adolescents, novice online users, and other vulnerable groups. Women who have formed half of the population in societies have an important role in cyberspace as in the real world. However, women are more exposed to violence in cyberspace than in the real world due to the absence of law and the power that supervises these users. Therefore, there is no gender equality despite all the efforts of international organizations and governments in elevating the position of women and creating gender equality in the real world. Women in cyberspace are exposed to different types of violence, including cursing, humiliating, threatening, and sexual stalking [26]. "Women need security in both the real world and cyberspace; however, this security need is sometimes neglected in cyberspace, unfortunately. Some examples of insecurity include verbal and written violence which are used online and in chatrooms as written attacks, using vile and hurtful words against women, or degrading and attacking the women's website to apply violence and demonstrate power against them. The existence of pornographic pictures on the internet trains men that women are vulnerable and must be abused and exposed to aggression, sexual assault, and harassment. Pornographic activities are a sign of continuing the patriarchal system since men desire to demonstrate their predominance to women via sexual abuse of women overtly and covertly, and these images exhibit women as obedient and submissive. Violence and sex are the main consequences of pornographic images. In most of these images, the men are dominant over women, and in the scenes, women are in worthless positions". A high percentage of female victims and male stalkers in the past 10 years has continuously proved that women are the most vulnerable targets in cyberspace crimes. For instance, the findings of a 10-year research show that:

In 2000, among 353 victims, 87% were female and 13% were male, and in 2001, 79.3% of the victims were female, and 16% were male among 256 victims; however, 58.6% of the stalkers were male, and 32.5% were female. In 2002, among 218 victims, 71% were female, and 28% were male; nonetheless, 52% of the stalkers were male, and 35% were female. In 2003, among 198 victims, 70% were female, and 27% were male; nevertheless, among stalkers, 52.5% were male, and 38% were female. Further, in 2004, among 196 victims, 69% were female, and 18% were male; however, among stalkers, 52.5% were male, and 23.5% were female. This unequal ratio between victimized and stalker men and women continued until 2010, when among 349 victims, 73% were female, and 27% were male, and among stalkers, 44.5% were male, and 36.5% were female [27]. The analysis of other statistics reveals that of every five victims, four of them are women, and women are exposed to cyberstalking eight times more than men [28]. In social networks, women are victimized by abusers who can be one person or a group of people with various methods. The abuser can be a man or woman, and these crimes might be due to sexual or non-sexual features. Almost, 50% of cyberstalking includes cases that the victim has first started an innocent and simple relationship on the internet [18]. Another research [28] stressed that single women are the main targets of cybercrimes, such as cyberstalking, desecration, extortion, impersonation, emotional deception, psychological damage, and so forth. The type of being victimized depends on various factors, including ideology, marital status, vocation and professional responsibilities, selected groups, cyber friends, language, and so on.

8. Policy Strategies for Cyberstalking

The incidence of cyberstalking depends on various factors, such as facilitating features and the absence of monitoring in cyberspace. Therefore, effective policies for cyberstalking require paying attention to the situation and features of criminal and victim parties and considering the features and variables in cyberspace. Identifying different types of disruptive-kind behaviors and criminology that fit into behavior should be regarded as the first effort by policymakers to fight harassment in cyberspace. Differential aggravated criminalization against vulnerable victims and numerous criminals should be considered as another approach in policymaking.

8.1. Recognizing and Criminology of New Disruptive Behaviors with Cultural Considerations

Recognizing every criminal event is the first step to making policy to fight crime. The absence of criminal protection and legislator's criminology are the reasons for numerous disruptive behaviors in cyberspace. The rapid emergence of new crimes in cyberspace and the continuous birth of criminal activities highlight the critical need for timely identification of offenses. Punitive measures may not be very effective, if the identification of harassing behavior in cyberspace as a crime occurs after it has become widespread among users. Therefore, timely criminalization is necessary. An important point to emphasize here is that for effective and proportionate criminalization of new offenses, it is crucial for lawmakers to consider the specific platforms within cyberspace where these crimes are most prevalent. Or, what gender and age range do the offenders belong to, and what personality types do they exhibit? Because combating crimes committed through email versus those on social media platforms involves significant differences, attention must be paid to distinctions in age, gender, and personality types of offenders.

Another point is the importance of cultural considerations in criminalization. For example, Iran's legislative approach to criminalizing cybercrimes has led to inadequate support for women. In many Western societies, the general culture does not classify many undesirable behaviors against women as crimes. For example, in these countries, the use of female models on adult websites, especially when the site displays the model with the consent of the woman, does not impose any criminal liability on the website operators. The authors of the European Union Convention and leaders worldwide, who are part of the EU Convention, have never considered women being harassed in cyberspace as a matter as significant as other crimes such as hacking.

8.2. Aggravated-Differential Criminalization

Criminal policy dictates that enhancing penalties for certain crimes better ensures the prevention of offenses. This measure is a specific form of aggravated-qualifying offense that considers the victim's circumstances and seeks to provide criminal support for them. Aggravation penalties sensitive to the gender and age of victims, whereby crimes against specific categories of victims receive harsher punishments, are an effective tool for controlling crime rates. Because such penalties deter criminals from committing crimes against these specific categories of victims. In fact, legislators can differentiate criminal behaviors against women through separate criminalization and impose differential punishments accordingly. Or at least, under those criminal titles, they can aggravate the penalties for these crimes when the victims are women. Furthermore, children as silent and vulnerable victims of cyberspace deserve greater legislative protection. Many of these victims may not even fully comprehend that they are being targeted by criminal acts, let alone seek legal prosecution for such actions.

8.3. Paying Attention to the Needs of the Victim

The first demand for the victims of harassment-based crimes in cyberspace is to accept their victimization since thinking of victims' experiences with doubt converts the bitter end of experienced pain into an endless bitterness of secondary victimization [29]. The victim must restate their story several times. Accordingly, there are many considerable therapeutic reasons in this case [30]. Cyber victims have more suppressed pains due to the virtual nature of the crime and the invisibility of victimization; thus, they naturally need to be heard more. It is highly influential for the cyber victim who feels more oppressed to restate his/her story of being victimized by the person or people who have victimized him/her.

The authority of the victim in determining the method of compensation supports the victim in controlling and minimizing the impacts of victimization. Perhaps the symbolic aspect of compensation that guarantees accepting guilt by the criminal encourages the victims of harassment-based crimes to prefer compensation to punishment. There are various options for compensation. Regarding harassment-based crimes that target the spiritual personality of people in crime, apologizing in the place of crime commitment and restoring the dignity of the victim are some parts of the victim's need for

justice execution. In addition, sending these mentioned cases to all the users who were present in the place during the crime or were in the process of crime is another part of justice execution.

8.4. Balanced Filtering of Platforms for Committing Crimes

Using filtering tools or refinement of cyberspace is considered an effective policy for cyberspaces that are special places for committing crimes. These limitations do not have regional opposition, and they are the public demands as well. However, tasteful and unrestrained usage of filtering might provide crime commitment due to the absence of noble users. Besides, communication and social network filtering in cyberspace deprive a few healthy and cautious people of using these communication tools due to the numerous and comfort of using VPN. Moreover, this filtering causes underage criminals and users to enter this unhealthy cyberspace or expose them to victimization without monitoring other social users.

8.5. Adopting a Collaborative Criminal Policy and Attracting Non-Governmental Organizations

Due to the specific features of cyberspace, it is not sufficient to be confined to a legal criminal reaction against a range of harassment-based behaviors at all. Collaborative control and solidarity find their meaning and concept by social group collaboration that initiates the pursuit via disclosing, declaring crimes, and presenting a complaint by organizations, associations, or syndicates [31]. Fortunately, Article 66 of Criminal Procedure Law approved in 2013 has taken an important action in establishing collaborative criminal policy in the discovery stage and prosecution of crime. Although this article has not named other organizations that have been activated in the field of cyberspace in a specialized way, it can include a high percentage of harassment-based behaviors due to the victimization of women and children. Allowing to declare crime, and present evidence and objection to jurisdiction by non-governmental organizations reduces the burden of the court on cybercrimes. Further, these two provide the opportunity to pursue cybercrimes by private prosecution organizations that have consisted of skillful people in terms of cybercriminal investigation by the advent of technical and specialized organizations. The most influential advantage of this approach is updating the methods of criminal prosecution and accelerating updating technical information and scientific exploration of crimes.

8.6. Supplying the Users with Supervisory, Technical, and Situational Prevention

Destructive disruptive behaviors, such as viruses and communication and telecommunication device disruptors are quickly spreading among a wide group of cyberspace users. Viruses and computer worms have the capability of procreation and exponential reproduction; thus, it is highly probable that victimization will happen again by spreading the virus. Comprehensive distribution and access to antivirus programs among users and supplying coping programs for them prevent the spread of reparation for the victim in addition to inhibiting victimizing others.

Rethink is a simple solution that prevents cyber violence by asking adolescents to rethink about sending insulting messages actively. Rethink is a software that determines insulting messages, using sensitive-to-text filtering technology without reading the messages. This system shows a pop-up message to users, reminding them that their message is insulting and asking them to rethink about sending it. This action gives opportunity to the writer of the message to think about the message without preventing sending it and advising directly. The users can send their primary message if they desire; however, studies have reported that only 10% of these people act so. Rethink was designed by an adolescent named Trisha Prabhu by getting inspiration from committing suicide of an 11-year-old victim of cyber violence. Prabhu and her group conducted much research and found that using Rethink has reduced the violent messages by adolescents from 71% to 4%. Rethink is available now as a free application; besides, it can be used in schools [32].

Supervision policy is one of the prevention tools for cybercrimes. These policies are the tools and programs that are installed on systems and record all the network activities of people, such as their taps on the keyboard or the points on which they click by mouse [33]. In situational prevention, these methods are highly effective tools to explore cybercrimes; nevertheless, there is no doubt that the privacy of people will be interrupted in cyberspace by applying such methods.

Privacy and civil liberty are the most significant rights of all people which have been emphasized in both international documents and domestic laws to be protected and respected. The main purpose of privacy is to protect personality and human dignity. Whichever way to look at this subject, the right to privacy is a principle that must not be violable. The significance of privacy and civil liberties has been emphasized in cases 112, 17, and 18 of the

International Covenant on Civil and Political Rights [33].

8.7. Improving Media Literacy and Cultural Norming

The advent of new communicative technologies and their application in society have created deep changes and have influenced the way of thinking, mind, and consciousness of the audience, perception, literacy, and comprehension of humans about the world and surrounding subjects. Eventually, such technologies make humans a new person whose understanding of the world influenced by technology is different from what it already was [34]. Digital literacy is rehabilitating the users to use media consciously and actively. Developing and reinforcing the digital literacy of citizens to use cyberspace is a solution that can be more effective than filtering. The explanation of the culture of using cyberspace and promoting and internalizing this culture in society is the basic action that should be taken by using communication tools. Proper and appropriate usage of cyberspace is not only the protective actions and measures for staying safe from cyberspace dangers. However, the concept of internalizing the culture of using this space properly is more significant, and it means internalizing positive and legal thoughts and opinions about this space in society. This will result in the advent of efficient and helpful users in this space. In other words, the nature of cyberspace should demonstrate that society considers this space as a tool to help humanity in line with daily activities by using advertising and educational tools. Moreover, cyberspace should be defined as a facilitating and accelerating tool for society's activities.

The users' justifications about appropriate reactions to cyberspace decrease victimization probability to a great extent. It seems that silence and the absence of reaction to a started cyber stalking increase the possibility of neutralization and sterility. On the contrary, an imprudent reaction to the stalking encourages the stalker to continue his/her behavior even if the reaction is a declaration of disgust for the stalkers and their behavior (Figure 4).

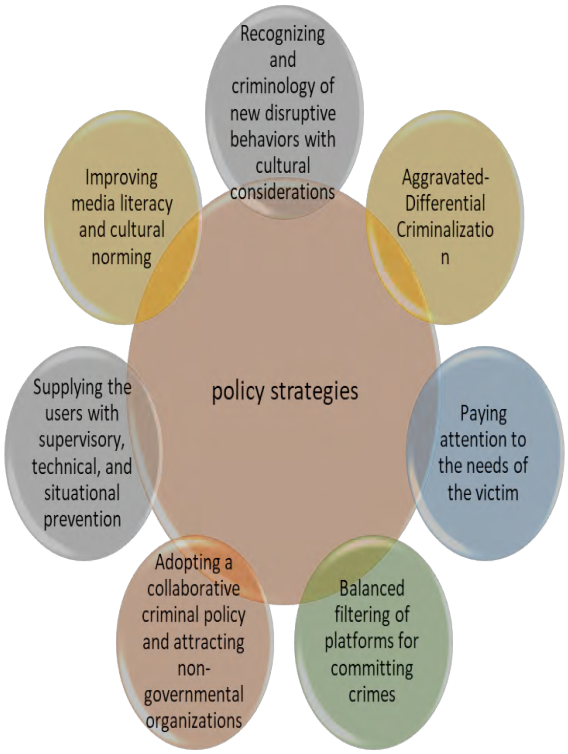

Figure. 4. Policy Strategies

9. Conclusion

The current study investigates the pillars, elements, and appendixes of cyberspace as a common crime in the space of cyber after stating the definitions and comparisons of cyberstalking. The types of cyberstalking have been classified into seven general categories, and it was clarified that cyberstalking is a public term for those crimes that target the spiritual personalities of other users. Such crimes include cyber gossip, cyberstalking, morphing, simulating and imitating, and cyberbullying (in a specific sense). Moreover, the most common tools and platforms for such crimes are social networks, emails, chatrooms, and some websites, respectively. The studies conducted on the motivation and features of criminals and victims of cyberstalking have reported influential results. The findings and statistics revealed that most stalkers are men; however, women are exposed to cyberstalking eight times more than men. Accordingly, it is highly necessary to make all efforts to recognize these crimes, criminals, and abused victims, and make policies in this regard to fight these criminal behaviors based on an accurate scientific base. These efforts should be made soon, considering all the mentioned issues, the obstacles to fighting these crimes, their novelty, publicization, and rapid progress in information and communication technology.

In a specific way, recognizing and criminology of new disruptive behaviors, differential aggravated criminology of crimes against women and children, and paying attention to the needs of the victim are some of the main policy strategies in line with knowledge enterprise response towards cyberstalking. Further, balanced filtering of platforms for committing crimes, adopting a collaborative criminal policy, and attracting non-

governmental organizations are the other main policy strategies. Finally, supplying the users with supervisory, technical, and situational prevention and improving media literacy and cultural norming are the last main strategies in line with the knowledge enterprise response towards cyberstalking. Eventually, for the research topic, it is recommended that active researchers in the field of cyberspace develop theories and executive mechanisms of these strategies, considering research on all the mentioned topics in the case of policy strategies.

Declarations

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

Authors' contributions

E.S: Data collection, analysis, manuscript drafting.
S.B: Data collection, article editing, Return the article to English.
P.D: Data collection, article editing, Return the article to English.

Conflict of interest

The authors declare that no conflicts of interest exist.

References

[1] K. Jaishankar, *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, CRC Press, 2011.

[2] R. Rosemary, A. B. Wardhana, H. M. Syam, N. "The relationship between anonymity and cyber sexual harassment by twitter users: a cross-sectional study," *Journal of Community Mental Health and Public Policy*, vol. 6 no. 2, pp. 95-104, 2024. https://doi.org/10.51602/cmhp.v6i2.131

[3] G. D. Walters and D. L. Espelage, "Assessing the relationship between cyber and traditional forms of bullying and sexual harassment: Stepping stones or displacement?," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 14, no. 2, 2020. https://doi.org/10.5817/CP2020-2-2.

[4] T. Vaillancourt., R. Faris and F. Mishna, "Cyberbullying in Children and Youth: Implications for Health and Clinical Practice," *The Canadian Journal of Psychiatry*, vol. 62, no. 6, pp. 368–373, 2017. https://doi.org/10.1177/0706743716684791.

[5] P. McDougall and T. Vaillancourt, "Long-term adult outcomes of peer victimization in childhood and adolescence: pathways to adjustment and maladjustment. *Am Psychol.*, vol. 70, no. 4, pp. 300–310, 2015. https://doi.org/10.1037/a0039174. .

[6] J. Wang, T. R. Nansel and R. J. Iannotti, "Cyber and traditional bullying: differential association with depression," *Journal of adolescent health*, vol.48, no. 4, pp. 415-417, 2011. https://doi.org/10.1016/j.jadohealth.2010.07.012.

[7] R. M. Kowalski, S. P. Limber and A. McCord, "A developmental approach to cyberbullying: Prevalence and protective factors," *Aggression and Violent Behavior*, 45, pp. 20–32, 2019. vol. http://doi.org/10.1016/j.avb.2018.02.009

[8] I. Zych, A. C. Baldry, D. P. Farrington and V. J. Llorent, "Are children involved in cyberbullying low on empathy? A systematic review and meta-analysis of research on empathy versus different cyberbullying roles," *The journal of aggression and violence*, vol. 45, pp. 83-97, 2018. https://doi.org/10.1016/j.avb.2018.03.004

[9] A. H. Najafi Ebrandabadi and H. Hashembeyki, *Criminology Encyclopedia*, Tehran: Ganj Publication, 5th, 2018. [In Persian]

[10] M. Shoaei and H. Khavaninzadeh, "Studying the Trend Analysis of Preventive Strategies of Cybercrimes," *Police Criminological Researches*, vol. 3, no. 6, pp. 185-209, 2022. https://doi.org/10.22034/cr.2022.1268358.1109.

[11] P. Bocij and L. McFarlane, "Seven fallacies about cyber stalking," Prison Service Journal, vol. 149, pp. 37–42, 2003.

[12] M. R. Davodi Farokhad, "The Article of Cyber Stalking," In *Encyclopedia of Cyber Behavior*, conducted by B. Shamloo, Mizan Publication, 2022. [In Persian]

[13] R. W. Leemis, D. L. Espelage, Basile, K. C. Mercer, L. M. Kollar and J. P. Davis, "Traditional and cyber bullying and sexual harassment: A longitudinal assessment of risk and protective factors across the social ecology," *Aggressive Behavior*, vol. 45, no. 2, pp. 181–192, 2019. https://doi.org/10.1002/ab.21808

[14] S. Low and D. Espelage, D. "Differentiating cyber bullying perpetration from non-physical bullying: Commonalities across race, individual, and family predictors," *Psychology of Violence*, vol. 3, no. 1, pp. 39–52, 2013. https://doi.org/10.1037/a0030308

[15] M. R. Davodi Farokhad, "Essay on Cyber Harassment," In *Encyclopedia of Cyber Behavior*, by B. Shamlou, Baqer, Mizan, 2022. [In Persian]

[16] M. Clemmitt, *Cyber socializing*, CQ Press, 2006. https://doi.org/10.4135/cqresrre20060728

[17] S. Hutton and S. Haantz, "Cyber stalking". Retrieved from, 2003. https://www.nw3c.org

[18] J. Reno, "1999 report on cyber stalking: A new challenge for law enforcement and industry," 1999. Retrieved from http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

[19] H. Tahan Nazif and M. Alipoor, M. "The Legal Position and Effects of Self-regulation of Digital Platforms," *ModernTechnologies Law*, vol. 3, no. 6, pp. 127-141, 2022. https://doi.org/10.22133/mtlj.2022.366647.1131

[20] R.Vasanthi, M. M. Rathishesha, V. Vinodhini, G. Manivasagam, M. Sangeetha, and R. Hinduja. "IMPACT OF CYBER BULLYING ON WOMEN EMOTIONAL HEALTH," *Journal of Advanced Zoology*, vol. *45*, no. 3, pp. 686–693, 2024. https://doi.org/10.53555/jaz.v45i3.4067

[21] N. E. Willard, Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats and Distress, Research Press, 2007.

[22] D. Halder and K. Jaishankar, Cyber Crime and Victimization of Women: Laws, Rights, and Regulations, Hershey, PA, USA: IGI Global, 2010.

[23] H. Alipour, *Information Technology Criminal Law*, Khorsandi Publications, 1st, 2011.

[24] L. Owens, R. Shute, and P. Slee, "Guess what I just heard!" Indirect aggression among teenage girls in Australia," Aggressive behavior, vol. 26, no. 1, pp. 67-83, 2003.

https://doi.org/10.1002/(SICI)1098-2337(2000)26:1<67::AID-AB6>3.0.CO;2-C.

[25] E. Andreou, "Bully/victim problems and their association with copying behavior in conflictual peer interactions among school-age children," *Educational Psychology*, vol. 21, no. 1, pp. 59- 66, 2001. https://doi.org/10.1080/01443410125042.

[26] M. Fattahian, "Investigating the Global Reasons for Increasing Cyber Violence Against Women," *Ghanonyar*, vol. 3, no. 3, pp. 29-48, 2017. [In Persian]

[27] D. Halder and K. Jaishankar, *Cyber Crime and Victimization of Women; Laws, Rights, and Regulations*, Igi Global, 2011.

[28] M. T. Whitty, "The realness of cyber cheating: Men's and women's representations of unfaithful Internet relationships," *Social Science Computer review*, vol. 23, pp. 57–67, 2005. https://doi.org/10.1177/0894439304271536.

[29] M.H. Zaker Hossein, "International Conference on Restorative Justice and Prevention of Cyber Crime," Tehran: Mizan Publication, 2016.

[30] Z. Howard, "Little Book of Restorative Justice," Old Philadelphia Pike, Good Books, 2009.

[31] M. Delmas- Marty, "Large Systems of Criminal Politics," (translated by A. H. Najafi Ebrandabadi), Tehran: Mizan Publication, Press. 1st, 2002.

[32] H. Jalali Farahani and M. Monfared "Legal Protection of Cyber Victims," *Majlis and Rahbord*, vol. 20, no. 73, pp. 155-200, 2013.

[33] S. A. Jazayeri, M. Neematollahi and A. Amirian Farsani, "Prevention of Cyber Crimes and the Limitations that Control It," *Ghanonyar*, vol. 3, no. 12, pp. 9-24, 2019. [In Persian]

[34] A. Khaksar Azghandi, "Investigating the Relationship between Media Literacy and Victim Bullying," *Journal of Pouyesh in Education and Consultation (JPEC)*, vol. 5, no. 10, pp. 91-105, 2019. 20.1001.1.2783154.1398.1398.10.5.4

Ehsan Salimi is an Assistant Professor at University of Maragheh. With years of experience and expertise in the field, he has established himself as a pioneer in the study of cybercrime and its impact on society. Salimi's research focuses on understanding the different types of cybercrime, their prevalence, and the factors that contribute to their occurrence.

Sepideh Boozari is an assistant professor in the Law Department of Maragheh University. She has expertise in jurisprudence and Islamic law and has recently published articles on women's studies and cybercrimes.

Prviz Dehghani is an assistant professor in the Law Department of Maragheh University. He has expertise in the field of contract law and has valuable experience in the field of practical legal issues.