e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

The Growing Threat of Cyber-bullying in India

Dr. Kalpana Jamgade,
Asst. Professor,
Orange City College of Social Work, Nagpur
Mob. 7387712366

ABSTRACT

India, a rapidly growing country in the cyber world, faces a significant increase in cyber-crimes, particularly cyberbullying. With over 33% of children experiencing online bullying, India has the highest prevalence of online harassment. According to NCRB data, the number of cybercrimes grew by 63.48% from 2018 to 2019. This issue draws attention to the threats posed by strangers and impersonators, especially targeting children and young people. To address this, the government and organizations have established legal provisions, initiatives, reporting portals, helplines, and awareness campaigns. However, more work is needed to combat cyberbullying effectively. A systematic study is necessary to find real solutions and alleviate the pain and suffering caused by this social problem.

Keywords: Cause and Effects, Cyberbullying, Indian government initiatives and legal provisions, Methods

INTRODUCTION

Cyberbullying is the term used for offensive, undesired, unfriendly, and aggressive behaviour that is sometimes displayed in public and is carried out via online technology to intimidate and injure the victims. Cyberbullying can be defined as verbal or relational bullying accomplished using electronic or wireless media. This phenomenon is receiving more attention as a result of its expanding existence and serious effects. Bill Belsey, a Canadian, coined the term "cyberbullying," which has rapidly expanded, and researchers, schools, and parents are understandably concerned that this issue is expanding faster than they can adequately respond. Cyberbullying has emerged as a new type of violent behaviour in the context of electronic communication over the past 10–12 years as a result of the numerous communication opportunities that technological advancement in electronics has made possible, particularly among adults and younger adolescents. In July 2021, 4,80 billion people worldwide were on social media, which is almost 61% of the world's total population depicting an annual growth of 5.7% as 7 lakh new users join per day and according to a UNICEF poll, more than 33% ofyoungsters are reported as victims of online bullying in 30 countries worldwide.

An article published on a website with the title-Cyberbullying statistics 2022 states that India (37%), Brazil (29%), and the United States (26%), were the top three nations where parents claimed that their children had suffered from cyberbullying whereas Russia, Japan, and Chile had the lowest parent reports, with 1%, 5%, and 8% respectively. According to NCRB 2020, total 50,035 cases of cybercrime were registered. NCRB data reported that cybercrimes in India have increased by 63.48% (27248 cases to 44548 cases) from 2018 to 2019 and 44548 cases to 50035 cases, which upsurged by 12.32% in 2020. Among these registered cases, 1614 cases were of cyberstalking, 762 cases were of cyber blackmailing, 84 cases of defamation, 247 cases of fake profiles, and 838 cases were of fake news. McAfee report published on Business Standard gives

e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

the updates on the recent year 2022, it states that India reported prominent acts of cyber-bullying such as: spreading false rumours at (39%), being excluded from groups and conversations at (35%), name calling at (34%). And according to Indian parents about 42% of children have been the target of racist cyberbullying, 36% have faced extreme forms of cyberbullying reported besides racism including trolling, 29% have faced personal attacks, 30% have been sexual harassment, 28% got the threat of personal harm and Doxing (23%), all of these at almost double the global average.

Problem Statement and Method: The rise of digital platforms has facilitated online harassment, leading to mental health issues and academic decline. Limited researches hinder effective solutions. Urgent action is needed through comprehensive research, policy development, and community engagement. Strengthening legal provisions, raising awareness, promoting digital literacy, and fostering collaboration among stakeholders are crucial. Addressing cyberbullying will create a safer online environment and protect vulnerable segments of society. This paper insights the systematic information on various social dimensions such as technology, communication, psychology, health, education, and youth development to enhance the understanding regarding cyberbullying with help of secondary data such as journals, magazines, publications, reports, books, articles, research papers, websites, manuals, booklets etc.

DIFFERENCE BETWEEN BULLYING AND CYBERBULLYING

Bullying and cyberbullying can be sub categorized into four major categories based upon the intentions, cause and effects, like physical, verbal, social and psychological. Table 1 lists these two forms of crime, bullying and Cyber Bullying through their typologies.

Table 1: Difference between Bullying and Cyberbullying

| SI.No. | Bullying | Cyber bullying |
|--------|-------------------------------------|---|
| 1 | Physical (Harm to the victim | Happy beating(Record a physical assault on a person and |
| | and/or her/his property) | spreading it on social networks) |
| 2 | Verbal(Insulting the victim) | Electronic insults(In public chars or via personal e-mails) |
| 3 | Social(By isolating the victim from | Harassment(Sending offensive messages on social |
| | group) | networks) |
| | | Denigration(Repeatedly broadcasting offensive |
| | | messages/pictures on social networks) |
| | | Disclosure and Hoax(Filtering of victim's compromised |
| | | information on internet/social media sites) |
| | | Cyber pursuit(Repeatedly sending threatening messages) |
| 4 | Psychological(Damaging the | Impersonation(Usurpation of the victim's identity on |
| | victim's self-esteem/ creating | internet/social media sites) |
| | insecurity or fear) | |

METHODS OF CYBER BULLYING

Flaming: Flaming is the term for furious, hostile texts that frequently use inappropriate words and sexual content. Flaming frequently happens in online conflicts and can lead to a "flame war." **Harassment:** Email, text messages, instant chats, bulletin board postings, and chat rooms can all be used as methods of harassment. It entails sending insulting or nasty texts continuously.

e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

Denigration: Denigration is the act of making disparaging remarks about the target and spreading them online. The claims are frequently made in order to harm the target. The goal is to damage the target's reputation or friendships.

Masquerading: Advanced technical abilities are needed for masquerading. The bully impersonates the target and sends hurtful communications that seem to be coming from the victim.

Outing and trickery: Trickery and outing frequently go together. The bully coerces the target into revealing details or making claims, which the bully subsequently makes public in an effort to make the target look bad. This is the method used by former friends to leak confidential information or humiliating pictures.

Impersonation: In order to harm the victim's reputation, the bully would impersonate the victim online by making a fake profile or claiming to be the victim while saying hurtful things.

Social exclusion: Online social isolation is just as real as it is offline. Targeted people are either left off of different "buddy" lists or are not permitted entry into chat rooms.

Causes of Cyber Bullying:

The study shows that relationship issues, such as breakups, envy, intolerance, and grouping together, are the most frequent causes of cyberbullying.

- 1. Lack of parental control over children's computer and internet use.
- 2. Insufficient computer or internet experience
- 3. Distinctions in race, culture, or religion between the offender and victim
- 4. Both bullies and victims have low self-esteem.
- 5. Lack of understanding of proper internet behaviour.
- 6. There is no one element that directly causes bullying; rather, a number of risk factors combine to raise the chance of bullying.
- 7. There are several possible risk factors that might influence whether or not kids become bullies or victims.
- 8. Bullies are more likely to be male, in lower grades, and to have other bullies as pals. Victims typically originate from dysfunctional households.
- 9. Another risk factor for both bullies and victims is low self-esteem.

Effects of Cyber Bullying:

Victims also experience severely detrimental effects, particularly to their social well-being, and schools and students' response is frequently inappropriate, non-existent, or ineffective. However, the consequences experienced by cyberbullying victims vary in severity based on a variety of contextual elements, such as whether anonymity exists or not or the presence of onlookers. For instance, if victims of bullying experience increased discomfort, this anxiety is exacerbated in cases of cyberbullying since the victims are unaware of the identity of the bully and believe that anybody may be the perpetrator. It is also a significant psychological issue since there may be much more victims of cyberbullying than conventional bullying, which makes feeling exposed and like others may see them one of the most unpleasant elements for sufferers. Among the effects caused by cyberbullying, the following stand out:

e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

Physical: Headaches, stomachaches, restless nights, fatigue, backaches, lack of appetite, issues with digestion, etc.Emotional and psychological: Fear, including emotions of panic, tension, worry, sorrow, melancholy, and depression symptoms, as well as more frequent suicidal thoughts; More precisely, it was discovered in a recent meta-analysis that people who experience cyberbullying are 2.5 times more likely to actually commit suicide and twice as likely to have suicidal thoughts as those who do not.

School-related: One impact of cyberbullying is a lack of motivation for learning, which results in issues with academic achievement.

Psychosocial: Increased emotions of loneliness, ostracism, and perhaps social rejection.

These impacts are especially detrimental because they target the social centre of the person, which includes psychological needs like identity, belonging, and self-esteem.

Core elements of cyber bullying

Intention: In general, the intention is also a keystone concept in criminal law. In order to, convict someone of a crime, it is necessary to prove both that they committed wrongdoing and that they did so, or a guilty mind. As a result, several state cyberbullying statutes now mention deliberate actions. For instance, "the delivery of any electronic textual, visual, written, or spoken message with the malicious and purposeful aim to compel, abuse, torture, or frighten a person" is an example of cyberbullying. Intent is another essential factor that sets cyberbullying apart fromother harmful online behaviours, although it can be challenging to account for in operationalizations.

Repetition: Perhaps the most significant and recognizable aspect of bullying is repetition. For instance, most people would concur that it is not bullying if two people bump into each other accidentally once in a school corridor (even if aserious injury is involved). In a similar vein, punching someone in the nose only once-never again-is not bullying; it may be assault, in which case the offender is certainly deserving of punishment, but it is not bullying. In that it makes the target feel as though more assaults are about to happen, bullying is a particular and distinctive type of cruel action. The target, then, is constantly concerned about what the aggressor will do since bullying is continual.

Harm: In bullying incidents, the person being targeted has to be harmed in some way. The harm could be physical, emotional, psychological or behavioral. The presence of harm must exist in some form, even though it is sometimes harder to detect and quantify, especially in online situations. While the target's experiences are used to evaluate harm, the aggressor's perspective is used to determine intent.

Imbalance of power: Popularity, physical strength or size, social aptitude, quick wit, extroversion, confidence, IQ, age, sex, race, ethnicity, and financial standing are just a few traits that might provide an attacker perceived or actual influence over a target. It is possible that illintentioned remarks or a humiliating post from an aggressor who is physically stronger than the target cause more harm than if issued from an aggressor who is weaker than the target because of the possibility of real-world bullying (since most targets know their aggressors in real life).

Review of theoretical studies on bullying and cyberbullying:

e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

The key conclusions are that one in 3 children engages in some kind of bullying, and one in five kids engages in some kind of cyberbullying. Despite having negligible or insignificant effect sizes and a weak association with age, boys are more involved than females. Bullying and cyberbullying frequently overlap, and it is a significant issue for minorities.

The findings indicate both risk and protective variables for bullying and cyberbullying, as well as immediate and long-term grave repercussions. Although the impact sizes are minor and vary on the programme elements, anti-bullying treatments are often beneficial in decreasing bullying. Strategies for evaluating bullying and cyberbullying need to be improved. Bullying and cyberbullying are influenced by personal and environmental risk and protective factors. It is challenging to determine the cause of these relationships given that the majority of research are correlational. However, even without being able to prove causation, understanding these linkages offers helpful insights for comprehending and minimising the phenomenon.

Cyberbullying perpetration is related to moral disengagement. Bullying and cyberbullying are pervasive, there is a wide range of information on their specific, contextual, risk, and protective factors, and the repercussions are severe for all the pupils involved in the phenomenon. As a result, it is not unexpected that several anti-bullying programmes have been carried out throughout the globe and that numerous systematic reviews and meta-analyses have compiled evidence on the subject.

Prevention of Cyberbullying and Face its Negative Effects:

School intervention: In Flanders (Belgium), a study of 308 principals of primary and secondary schools indicated that most schools believed cyberbullying to be a serious issue, and that it was their responsibility to educate pupils about the issue and assist in finding solutions. They said that they would welcome scientific intervention and programmes with empirical support in addition to asking for professional assistance.

Family involvement: It is crucial that parents watch over how their kids use the internet and other technology. Additionally, they must keep an eye out for any mood swings their kids experience after getting a message or phone call, or when they use the Internet, since these might be signs of cyberbullying issues.

Psycho-social interventions: Social support, a sense of self-efficacy, the victims' social capital, their empathy, improving self-esteem and moral involvement, and self-esteem are all examples of psychosocial interventions. These require the addition of one more personalized element, namely the capacity to employ problem-centered coping mechanisms.

Increasing and strengthening social support: It is one of the most important ways to stop cyberbullying and lessen its effects, especially in light of the fact that teens who have been bullied online are more likely to turn to friends for support than to parents or teachers. This is because they feel disconnected from adults and believe that adults are the ones who can solve their problems. **Encouraging empathy and moral engagement:** If moral disengagement is a risk factor in bullying and cyberbullying, then moral engagement in and empathy with others will be relevant prevention factors.

Although there haven't been many studies on the effectiveness of different coping mechanisms in cyberbullying situations, they are becoming increasingly common.

e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

Victims of cyberbullying respond differently:

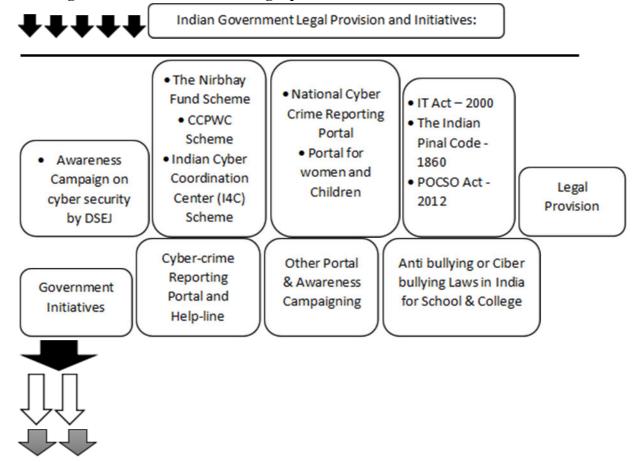
- Reactions that target the cyberbully, such as seeking retribution and defending oneself.
- Those that imply ignoring the aggressor.
- The sort that asks for help (from peers, parents, or teachers).
- Those who try to disable the bully's account through sophisticated cybernetic methods

Myths about Cyber Bullying:

There are various types of myths prevailing in present time related to Cyber bullying. Some of these are as follows (Sabella et al., 2013):

- Everyone knows what cyberbullying is? (due to improper definition)
- Cyberbullying is a rite of passage for all teenagers, just like conventional bullying is (it will give him/her a backbone so they can manage life).
- Bullies are cruel children or social misfits.
- Turn off your computer or mobile device to eliminate cyberbullying

Indian government initiatives and legal provisions:



(Fig 1: Indian government initiatives and legal provisions)

The Indian government has implemented several initiatives to combat cybercrime and deliver justice to victims.

Legal provisions:IT Act, 2000: In order to guarantee legal identity for the electronic interchange of data, the IT Act of 2006 came into effect. Up to three to five years in jail and a fine of one lakh

e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

rupees, or both, may be imposed for computer-related offences, and in extreme circumstances, even more. Sections 66A, 66C, 66D, and 66E of the IT Act impose penalties on anybody found guilty of an offence involving disrespectful behaviour online, on social media, or with other digital media. IT Act sections 67, 67A, and 67B address the publication and electronic transmission of content involving sexually explicit acts, etc.

POSCO Act 2012: Protection of children from sexual offenses (POCSO) is a comprehensive regulation that guards against the horrible actions of sexual assault, sexual harassment, and pornography for minors under the age of 18.

Link: https://legislative.gov.in/actsofparliamentfromtheyear/information-technology-act-2000

The Indian Penal Code: The Indian Penal Code (IPC)7, was created in 1862 during all British Presidency, is the country's official criminal code and deals with all substantive areas of criminal law.

Table 2: IPC Sections and types of cyberbullying

| Sl.No. | IPC Sections | Туре |
|--------|--------------|---------------|
| 1 | 292A | Black-mailing |
| 2 | 354A | Harassment |
| 3 | 354D | Stalking |
| 4 | 499 | Threatening |
| 5 | 507, 509 | Intruding |

Government initiatives

The Nirbhaya funds scheme: It is an initiative of the Government of India under the Nirbhaya funds scheme for ensuring the safety of women and children (2013). The ministry of Home affairs generated a single number (112) which was under the Emergency response support system (ERSS), to cope with any emergencies where immediate assistance from police, fir, and rescue, or any other help is required.Link: https:// 112. gov. in/

Cyber Crime Prevention against Women and Child: The CCPWS system establishes several sections that are in charge of reporting online criminal actions and related investigations, examining complaints of cybercrime, and spotting any concerning cybercrime circumstances.

The scheme has an estimated outlay of Rs. 223.198 crores overall, and its key components are listed below:

- Online cybercrime reporting platform
- > One national level cyber forensic laboratory
- > Training of Police officers, judges & prosecutors
- > Cybercrime awareness activities
- Research & Development

More than 3800 complaints were received on www.cybercrime.gove.in in the year 2019.

Indian cybercrime coordination centre (I4C) scheme:

I4C serves as a crucial weapon in the battle against cybercrime to deal with all forms of cybercrime in the nation in a coordinated and all-encompassing way, preventing the needless use

e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

of social space. Additionally, it is aided in working on many projects by multinational organisations and the rapid growth of technology. Its goal is to address a variety of concerns raised by internet media, with a focus on victims who are women and children. It also aims to raise awareness among young people and encourage the quick reporting of financial frauds in order to deter thieves from stealing money.

Cybercrime reporting portals & helplines:

National cyber-crime reporting portal: The NCCR site is a government of India programme that allows victims of criticism, particularly women and children, to register online complaints. They respond to complaints as soon as they are made, with the support of the local police. Technology currently outperforms all conventional methods and is quicker than the offline process for reporting cybercrime. The National Cyber Crime Reporting Portal allows for the registration of cybercrime complaints, which enables the filing of complaints about cybercrimes across the country and allows victims and complainants to easily access cybercrime cells and all relevant information. The victim of a crime can also registers with a nearby cyber-crime cell as an alternative to making a formal complaint. Cyber Crime Portal State-wise, Nodal cyber cell officers and grievance officers' contact details and e-mail IDs are provided on the website https://cyber-crime.gov.in/.

Table 3: Portal for women and children

| Sl.No. | Portals | Description | |
|--------|-------------------------|---|--|
| | National women helpline | 181 is the number for the national women's helpline. | |
| | number 181 and e-mail | Additionally, a special e-mail address called Complaint- | |
| | | mwcd@gov.in has been established for women and children to | |
| | | use when reporting cases of abuse, harassment, and offensive | |
| | | social media content. | |
| | Childline 1098 | In accordance with the National Commission for Women Act of | |
| | | 1990, the National Commission for Women was established to | |
| | | review the constitutional and legal protections for women and | |
| | | to make recommendations for corrective legislative actions. | |
| | | Additionally, a helpline was established to provide women with | |
| | | a digital complaint registration system. Moreover, it aids in the | |
| | | resolution of any disputes and provides government advice on | |
| | | all issues of policy that impact women.Link: | |
| | | http://www.ncw.nic.in/helplines | |
| | Mahila-Bol help-lined | In December 2017, Mahila-Bol started in India in partnership | |
| | number: | with the Government of India and the United Nations to end | |
| | 01244007444 | the menace of sexual harassment of women in the | |
| | | workplace.Link: https://mahilabol.org/women-helpline/ | |

Anti-bullying or cyberbullying laws in India for schools and colleges:

The HRD ministry has established anti-ragging committees in response to the sharp rise in bullying in schools, particularly in boarding institutions in India, in an effort to lower the incidence of bullying. These committees focus on disciplining students who participate in these

e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

activities, which may include rustication in cases of significant bullying activity. With proper UGC policies on reducing the prevalence of ragging in higher institutions, the University Grants Commission announces anti-ragging measures for universities and colleges.

Other portals & awareness campaigns:

The Ministry of Home Affairs established a centralised online cybercrime reporting platform, enabling victims to file a complaint without going to the police station. Additionally, the Delhi, Indore and Uttarakhand police have a cyber squad to inform people about submitting a complaint online by visiting the following link:

- > http://www.cybercelldelhi.in/
- > http://www.indorepolice.org/cyber-crime.php
- > https:// ifflab. org/ how- to- file-a- cyber- crime- complaint- in- india/
- > https://uttarakhandpolice.uk.gov.in/services

Awareness Campaign on Cyber Security:

On January 15, 2021, DSEJ sponsored a large-scale awareness campaign on cyber hygiene and security for up to 2 Lakh stakeholders in the School Education Department. This campaign included both online and offline counseling sessions that covered a variety of topics.

- > Cyber grooming,
- > Cyberbullying, phishing,
- > Safeguarding social media accounts,
- > Online banking frauds,
- > Lottery frauds, remote access scams,
- > Social media privacy policy, etc.

Facts about Cyber bullying:

- Over one-third of all students experience cyberbullying.
- Social media is the most popular venue for cyberbullying.
- Nearly 25% of students admit to acting cruelly.
- Girls experience cyberbullying the most frequently.
- The majority of people who see cyberbullying do nothing.
- Using a smartphone is associated with an increase in cyberbullying.
- Cyberbullying frequently occurs in online gaming.
- Rates rise by more than 50% for LGBTQ+ students.
- Cyberbullying increases the suicide risk among young people.
- Parents, teachers, administrators, and youth can help stop cyberbullying.

The non-governmental organisation Child Rights and You (CRY) conducted a study titled "Online Study and Internet Addiction," which was published on February 18, 2020.In Delhi-National Capital Region, 630 teenagers were surveyed, and 9.2% of them reported cyberbullying, but half of them didn't tell anybody about it. Online bullying was a risk for 22.4% of respondents (aged 13 to 18) who spent more than three hours per day online. Over four hours per day were spent dealing with cyberbullying (28%). A modified image or video of oneself was also reported by one in four teenagers, and 50% of these incidents were not reported to the authorities.1stCase of cyberbullying in IndiaRitu Kohli, a young woman, complained in 2001 that someone was

e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

impersonating her identity on social networking and that she was purposefully receiving calls from several numbers, including calls from abroad. Additionally, a case was brought under Section 509 of the Indian Penal Code. Manish Kathuria, the case's offender, was taken into custody by the Delhi Police. In the aforementioned instance, Manish engaged in illicit communication with Ritu Kohli on the website http://www.mirc.com while tracking Ritu Kohli online. The case of Ritu Kohli served as a warning to the government to enact legislation outlawing the above-mentioned crime and providing for the protection of victims. As a result Section 66A of the Information Technology Act, 2008 (ITAA 2008) states, "Punishment for sending offensive messages through communication service, etc".

CONCLUSION

Nowadays, the Internet is the primary means of contact among people. However, very few studies on the relationship between cyberbullying in teenagers and cyberbullying in adults have been conducted. Cyber violence victimization can cause the individual to get isolated from the environment which leads to social, emotional, and intact mal-adjustments. Cyber-bullying victims have significantly higher depression, anxiety, and stress levels compared to non-victims. Symptoms of social, emotional, and incestual maladjustments are low self-esteem, anxiety, anger, mood disruptions, depression, and school absenteeism. Poor grades, an increased tendency to violate each other, and youth suicide. Government is also playing a significant role in creating a healthy environment for all. Awareness must be developed among administrators, teachers, parents, students, mass media, and whole community members of this universe regarding these issues. Self-awareness and motivation are the keys to this problem. If the proper rules, and other remedies are followed we can over-come from the manacel.

REFERENCES

- "Internet organized crime threat assessment", Technical report, Europol, 2016.
- James Comey, "Worldwide threats to the homeland: ISIS and the new wave of terror, statement before the house committee on homeland security", FBI, July 2016.
- "Internet security threat report", Technical report, vol. 21, Symantec, April 2016.
- Nahal Sarbjit, Ma Beijia, Tran Felix, "Global cybersecurity primer", Technical report, Bank of America Merrill Lynch, 2015.
- Nabie Y. Conteh, Paul J. Schmick, "Cybersecurity: risks, vulnerabilities & countermeasures to prevent social engineering attacks", International Journal of Advanced Computer Research, Vol. 6 pp.23-31, 2016.
- "State of cyber security implications for 2016", Technical report, ISACA and RSA, 2016.
- "The human factor", Technical report, Proofpoint, 2016.
- Kevin D. Mitnick, William L. Simon, "The art of deception: Controlling the human element of security", John Wiley & Sons, 2011.
- "Hacking the human operating system: The role of social engineering within cybersecurity", Technical report, Intel Security, 2015.
- Prashant Kumar Dey, "Prashant's algorithm for password managementsystem", International Journal of Engineering Science, pp.2424, 2016.

e-ISSN No. 2394-8426

Special Issue on Cyber Crime and Social Media Issue-III(II), Volume-XIII

- Seppo Heikkinen, "Social engineering in theworld ofemerging communication technologies", Proceedings of Wireless World Research Forum, pp. 1-10, 2006.
- Rahul Singh Patel, "Kali Linux Social Engineering", Packt Publishing Ltd, 2013.
- Joseph Muniz, "Web Penetration Testing with Kali Linux", Packt Publishing Ltd, 2013.
- Andrea Cullen, Lorna Armitage, "The social engineering attack spiral (seas). In Cyber Security And Protection Of Digital Services (Cyber Security)", 2016 International Conference On, pp.1-6, IEEE, 2016.