ज्ञान-विज्ञान विमुक्तये

athshala पाठशाला

MHRD Govt. of India

athshala पाठशाला

A Gateway to all Post Graduate Courses

MHRD Govt. of India

An MHRD Project under its National Mission on Education through ICT (NME-ICT)

Subject: CRIMINOLOGY

Production of Courseware

- Content for Post Graduate Courses

Paper : CYBER CRIMINOLOGY & CYBER FORENSICS

Module : Moral Disengagement Theory and Cyber Crimes

ज्ञान-विज्ञान विमुक्तये

MODULE 27 : MORAL DISENGAGEMENT THEORY AND CYBER CRIMES

Component - I - Personal Details

Role	Name	Affiliation
Principal Investigator	Prof(Dr) G S Bajpai	Registrar National Law University Delhi
Paper Coordinator	Prof(Dr) K. Jaishankar	Professor and Head, Department of Criminology, Raksha Shakti University, Ahmedabad, Gujarat
Content Writer/Author	Amit Gopal Thakre	Trained Criminologist, Department of Criminology, Raksha Shakti University, Ahmedabad, Gujarat
Content Reviewer	Prof(Dr) K. Jaishankar	Professor and Head, Department of Criminology, Raksha Shakti University, Ahmedabad, Gujarat

Component - I (B) Description of Module

	Description of Module
Subject Name	Criminology
Paper Name	**Cyber Criminology and Cyber Forensics**
Module No.	27
Module Name/Title	**Moral Disengagement Theory and Cyber Crimes**
Pre-requisites	Psychology, Morality, Labeling, Cyber bullying, Social Networking Sites
Objectives	• To understand Moral Disengagement Theory. • To link Moral Disengagement Theory with criminal behavior in cyber space. • To study contributing components of moral disengagement theory from the perspective of cyber crime. • To understand decision making of cyber criminal based on moral disengagement theory.
Keywords	Moral Disengagement, Moral Justification, Euphemistic labeling, Advantageous comparison, Displacement of responsibility, Dehumanizing the victim.

Table of Contents

Learning Outcomes

After completing this module, you will be able to understand:

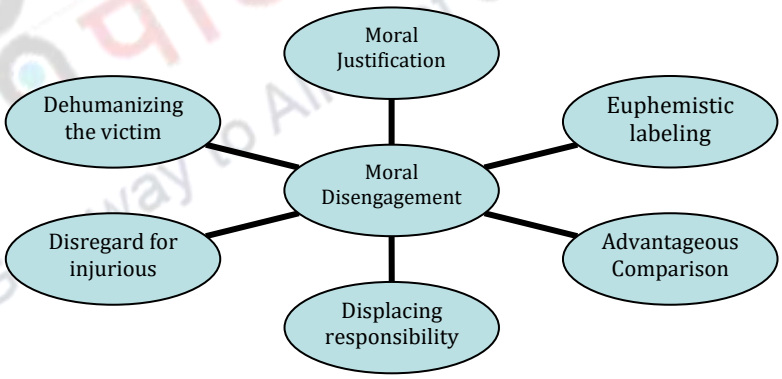
- The psychological process of a criminal based on the foundation of Moral Disengagement Theory.
- The psychology of a cyber criminal from the perspective of Moral Disengagement Theory.
- The psychological pressure behind cyber criminal due to contributing components of Moral Disengagement Theory.

Moral Disengagement Theory and Cyber Crimes

1. Introduction

Many psychologists explained the causes of criminal behavior hidden in psychological processes. One of such prominent psychologist is Albert Bandura who propounded Moral Disengagement Theory (MDT) to explain the psychological processes behind criminal conduct. According to MDT, just before committing the crime, the criminal detaches himself consciously from morality and this detachment is due to realizations that seemingly justify criminal conduct. This phase of detachment is temporary in nature by putting oneself in a state of mind where inhumane conduct is justified without any follow through leading to self-condemnation (Bandura, 1999). Commonly, people act in a way that gives them a sense of self-worth and satisfaction. This feeling of self-satisfaction comes when a person regulates himself as per internalized moral standards. The process of regulating self may not always be active because it is dependent on external (social) and internal (psychological) processes. The process of selective activation of self-regulation leads to diversity in people's behavior.

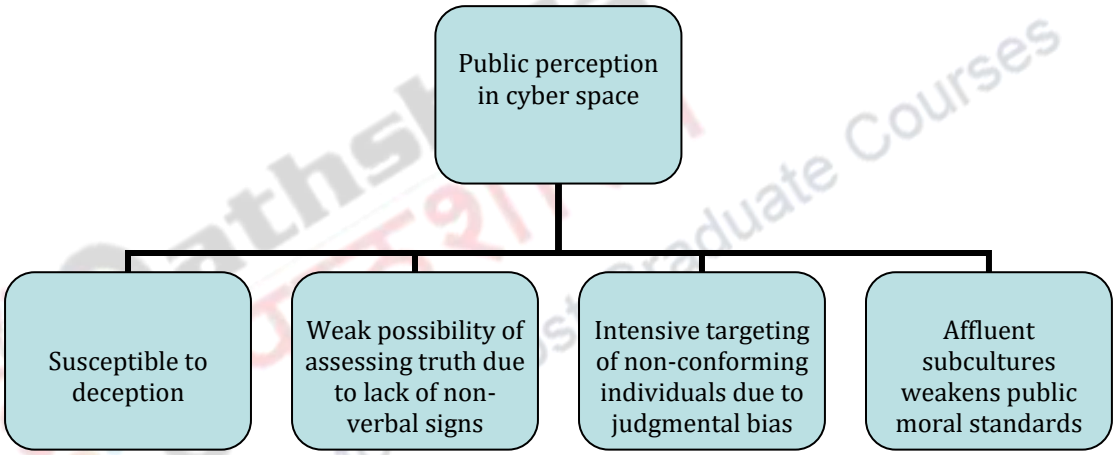
As per Bandura, moral disengagement happens through following reasons:



2. Contributing Components of MDT

The spike in cyber crimes in last few years is a cause of major concern and needs to be researched well. The key lies in understanding the behavior of cyber criminal which shall render ways to implement appropriate interventions. Moral Disengagement Theory is one such theory that assists in understanding the behavior of cyber criminals through its various contributing components. The contributing components of MDT as depicted in figure above are described below from the perspective of cyber crime.

1. *Moral Justification:* Bandura suggested that morally justifying the act of violating self-regulation is the first step of a psychological process in MDT. For example, harassing someone in social media because of victim's different opinion as against popular political scenario. Harassing and targeting such person also seem acceptable to a majority of people. In cyber space, victimization is rampant and obvious where there is a conflict between ideologies pertaining to religion, nationalism or sexual preferences. The interesting pattern is, MDT then moves on from individual level to mass level where cyberspace starts forming public opinion, resulting in masses to morally justify wrongful behaviors. Kathleen (1998) analyzed the process of structuring of public opinion and found that there are four factors that act as a source to moral disengagement at the mass level and which could also be applied to cyber crimes happening in cyberspace.

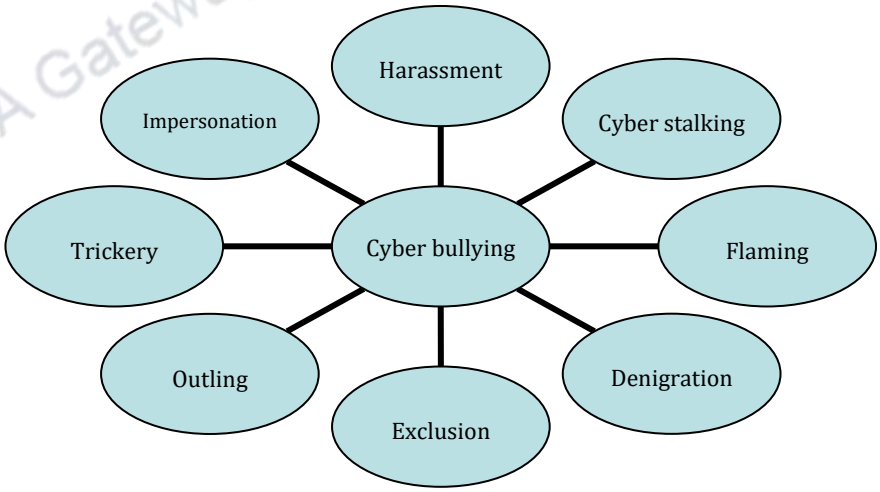


All the above factors are reinforcing agents for justifying immoral activities in cyberspace. It could be ascertained that people easily conforming to social arbitrary demands are more vulnerable to moral justification. This opens up the debate for a scope for the moral justification for people with high moral principles. It appears that the reason behind aggression of victim (with high moral principles) of cyber crime is their reverting back at times when their identity is challenged.

2. *Euphemistic Labeling:* Social networking sites serve as a garden for growing euphemistic subculture. It is a common practice by internet users to use euphemistic language to describe something wrongful. This is another way used by internet users to morally disagree with their principles. Regarding some serious social issues, adults usually express themselves aggressively by rephrasing and this makes them feel liberated from remorse (Diener, et al., 1975). The increased frequency of such behavior in short frame of time leads to trolling of targeted individuals which might have severe consequences on

victim's life. It appears that language sanitation has become an order of the day; severe acts of aggression are mellowed down through euphemism on social media to favorably mold public opinion. If we look at recent issues in public discourse, religious sentiments are exaggerated and portrayed to be under attack from other religion. Such tactics are used and found to be effective on social networking sites due to mass connectivity and have led to divide among people. The implication of this divide is evident in recent attacks on minority segment in India. The implication of euphemism subculture in virtual space might result in severe form of mass victimization in real life.

3. *Advantageous Comparison:* In this psychological mechanism, the individual compares his own wrongful act with others- bigger immoral behavior. This way the individual lower self-regulation by making his own act comparatively less wrongful (Bandura, 1999). This psychological process may also be adopted by the hackers who might justify their act as less harmful as compared to mass casualties happening across the world over. The crimes in cyber space could possibly be an outcome of utilitarian standards, for example, a cyber-terrorist may choose to deface a government website to send across a political message thinking that it is a better way to propagate an ideology without loss of human lives. There are certain forms of cyber crime wherein commonalities could be seen in terms of advantageous comparison, for instance, in cases of cyber bullying, harassment, cyber stalking or labeling in social networking sites to defame an individual. The cyber criminal may justify these actions by gauging them as less harmful as compared to inflicting physical harm to the victim. The various types of cyber bullying are illustrated in figure below.



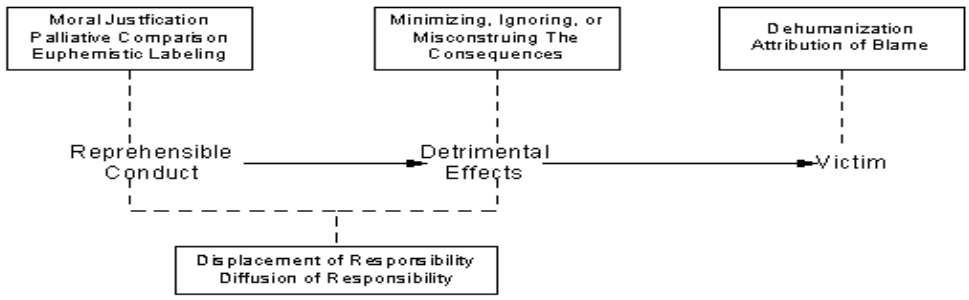
4. *Displacement of Responsibility:* The functionality of this mechanism depends on offender's ability to distort the connection between his actions and its consequences. This distortion is also justified by viewing the actions as legitimate under the authority. Here,

the authority shows the tendency to take the responsibility for individual's wrongful actions. The authority would create a sense of solidarity and emphasize on cumulative devotedness towards authority's objectives, henceforth diminishing the wrongful acts by an individual. State sponsored cyber attacks on a rival country are one such example where the cyber criminal do not feel as the true agent, rather takes his actions as a contribution to authority. Such kind of thought process saves the cyber criminal from self-condemnation. The same psychological mechanism could be applied to state-sponsored terrorism or an organized human/drug trafficking gang - operating online. The aforementioned organizations would employ devoted functionaries. The organization would create a subculture in which an individual would not have to worry about the consequences of his actions becomes the organization takes the responsibility of it. This further intensifies employee's devotion towards authorities.

5. *Disregard for injurious consequences:* Showing disregard for harm caused to others due to personal actions is a way of disengaging self from moral principles. Jaishankar (2008) in his Space Transition Theory (STT) explained about the behavior relating to repressed criminality emerging in cyber space. Second postulate of STT states that it is the identity flexibility, anonymity and low deterrence that motivate the offender to commit crime in cyber space and in such scenario it is easier to disengage self form the plight of the victim. Bandura (1999) also supports the idea of relative convenience for offender to commit crime when its consequences are not visible. In cyber crimes, the anonymity between victim and offender removes the factor of personal responsibility from the offender's psyche (by keeping offender unaware of harms faced by the victim).
6. *Dehumanizing the victim:* The offender tends to view victim sans human attributes. The victim is objectified as sub-human (Alleyne et al., 2014). Dehumanizing the victim makes it easier for the offender to validate wrongful treatment of the victim. It may also happen that a particular individual or a group may be excluded from the mainstream by justifying immoral act towards them. Zang et al. (2014) further illustrated on the human attributes that are majorly neglected by the offender when he thinks of a victim. These attributes could be unique to the individual (rationality, demeanor, attitude) or it could be characteristic (caring, emotional, openness to ideas). In cyber space, dehumanization could be exaggerated to group level wherein one social in-group may treat other as 'non-human' out-group with inferior human qualities. Such animal like treatment by in-group members makes them lesser compassionate towards out-group and increases the propensity of victimization of out-group by in-group.

3. Discussion

Researches have shown that computer criminals justify their actions by calling it 'an act for fulfilling higher moral principles' (Parker, 1998) or cyber criminal justify their means to reach an aim (Chantler, 1996). To reach these aims, the cyber criminal uses information technology for committing espionage, fraud, cyber terrorism, online/offline harassment, perversion and other crimes in cyber space (Clarke, 1998; Mizrach, 1997). The cyber criminals might also find solace in subculture wherein the acts of cyber crime are equated with 'being a watchdog/vigilant, doing social service, holding government accountable' (Rogers, 1999). The model diagram below shows the concept of Moral Disengagement Theory propounded by Bandura (1999).



Source: From Mechanisms of Moral Disengagement in the Exercise of Moral Agency (p. 365) by A. Bandura, C. Barbaranelli, G. Caprara, and C. Pastorelli, 1996, Journal of Personality and Social Psychology, 71.

Moral Disengagement Theory explains the behavior of hackers and cyber criminals who see their act as activism for open access to information for all. The persona of being a 'Robin Hood' in cyber space is acquired by majority of cyber criminals and this avatar is in turn promoting cyber terrorism and white collar crimes having real life implications. Moral disengagement theory can be used to understand the behavior of a cyber criminal with special reference to social networking sites. The subculture in cyberspace is fertile for promoting palliative comparisons or euphemistic labeling. Even though there are detrimental effects associated with such reprehensible conduct, the cyber criminal justifies his actions by minimizing or ignoring the consequences. When it comes to victimization, the offender detaches himself from the victim by dehumanizing the attributes of victim or place the blame on victim.

4. Summary and Conclusion

Recent years have shown sudden surge in masses relying on information technology that also led to increase in number of cyber crimes. As per Symantec Report on Cyber Security Threat, it takes only 2 minutes for an hacker to attack 'Internet of Things' that could have dreadful impact on lives of millions of people relying on the network services. The psychology of cyber criminal is intrigue and needs to be reviewed from the lenses of criminological theories. What makes a cyber criminal to cause harm in virtual world, even that do not involve monetary benefits for the criminal? How a cyber criminal manages to ignore the psychological impact left over the victim? Such questions may be answered by moral disengagement theory.

Moral disengagement theory explains the behavior of a cyber criminal. Interestingly, using moral disengagement theory to explain cyber criminal forms a unique linkage of cause and effect between 'the decision made in real life by the offender' with the 'consequences resulting from actions done in virtual world'. The mechanism of moral disengagement in cyber space happens through justifying the act of cyber crime, involving in euphemistic labeling in social networking sites, advantageous comparisons, displaying responsibility, having no regard for the victim's feelings and dehumanizing the victim.

References

Alleyne, E., Fernandes, I., & Pritchard, E. (2014). Denying humanness to victims: How gang members justify violent behavior. *Group Processes & Intergroup Relations*, *17*(6), 750–762.

Bandura, A. (1999). Moral Disengagement in the Perpetration of Inhumanities. *Personality and Social Psychology Review*, *3*(3), 193–209.

Chantler, N. (1996). *Profile of a Computer Hacker*. Florida: Infowar.

Clarke, R. (1998). *Technological aspects of internet crime prevention*. Retrieved from http://www.anu.edu.au/people/Roger.Clarke/II/.

Diener, E., Dineen, J., Endresen, K., Beaman, A. L., & Fraser, S. C. (1975). Effects of altered responsibility, cognitive set, and modeling on physical aggression and deindividuation. *Journal of Personality and Social Psychology*, *31*(2), 328–337.

Jaishankar, K. (2008). Space Transition Theory of cyber crimes. In Schmallager, F., & Pittaro, M. (Eds.), *Crimes of the Internet*. (pp. 283-301) Upper Saddle River, NJ: Prentice Hall.

Kathleen, M. (1998). Manipulating Public Opinion with Moral Justification. *Annals of the American Academy of Political and Social Science*, *560*, 129–142.

Keniston, K. (1970). Student activism, moral development, and morality. *American Journal of Orthopsychiatry*, 40(4), 577–592.

Mizrach, S. (1997). *Is there a hacker ethic for the 90s?*. Retrieved from: http://www.infowar.com.

Parker, D. (1998). *Fighting computer crime: A new framework for protecting information.* New York: John Wiley & Sons.

Rogers, M. (1999). *Psychology of hackers: Steps toward a new taxonomy*. Retrieved from: http://www.infowar.com.

Zhang, H., Chan, D K S., & Cao, Q. (2014). Deliberating on Social Targets' Goal Instrumentality Leads to Dehumanization: An Experimental Investigation. *Social Cognition*, *32*(2), 181–189.