VOL.6 ISSUE 2
DROIT PENALE: INDIAN LAW JOURNAL ON CRIME & CRIMINOLOGY
ISSN: 2456-7280

DIFFERENCES IN THE NEEDS OF VICTIMS OF CYBER DEPENDENT CRIMES: A PARADIGM SHIFT FROM COMMON NEED BASED APPROACH TO RIGHT BASED APPROACH

Leelesh Sundaram.B[1]

Abstract

The internet in India is developing quickly but significant weaknesses is Cybercrime – illicit activity carried out on the internet. The internet, alongside its focal points, has additionally presented us to security hazards that accompany interfacing with an expansive network. The government by virtue of affirmative action's has developed a common tool of restorative justice for victims of cyber dependent crimes. However, in the Indian jurisprudence, the restorative tool remains constant and the difference in the need of victims is unknown. since need based approach is followed, the difference in the need of cyber dependent crime victims is unknown. If there is difference in the need of cyber dependent crime victims, a conclusion that the current system is a failure could be made and the swift of approach becomes mandatory. Thus, this research aims in finding out difference in the need of cyber dependent crime victims. This empirical research is carried out with a sample size of 253 from a open sample frame determined through convenient sampling method. With the help of complex graphs, mann whitney u test, Jonckheere-Terpstra Test. The findings in the study finding permits to make a conclusion that there is difference in the need of cyber dependent crime victims, and the current system is a failure, the swift of approach becomes mandatory

Keywords: cyber dependent crime, victims, needs, approach, restorative justice

Introduction

The internet in India is developing quickly. It has offered ascend to new open doors in each field we can consider – be it excitement, business, games or training. There are two sides to a coin.

[1] LLM -Commercial Law, Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences , (SIMATS) Saveetha University, Chennai 77. Mail Id: leelesh03@gmail.com Ph.no. 9092289877

Internet additionally has its own particular drawback.. One of the significant weaknesses is Cybercrime – illicit activity carried out on the internet. The internet, alongside its focal points, has additionally presented us to security hazards that accompany interfacing with an expansive network. Computers today are being abused for illicit exercises like email undercover work, charge card misrepresentation, spams, programming theft et cetera, which attack our security and annoy our faculties. Cyber Dependent Crime is any unlawful conduct coordinated by methods for electrical activities that attempts to hurt the security of computer systems and the information prepared by them. In a more extensive sense, in any case, a computer related crime might be any unlawful conduct carried out by methods for or in connection to a computer system or network. Even subsequent to taking a few measures to stay away from computer crime and secure the computers, still computer crimes do happen sooner or later or other. Therefore most noteworthy need ought to be given to aversion.

The government has taken various steps towards curbing of offences which are cyber dependents. The recent amendment in criminal law and Information technology Act has tried its level best to curb the increasing rate of offences and offer protection to the victims. Various efforts are taken by the government to reduce chances of victimhood and victimization through awareness and imposing regulations in the form of restrictions At the same time various government institutions including the CBI have attempted to identify the reason for occurrence of cyber crimes and in particular to social networks. The government by virtue of affirmative action's has developed a common tool of restorative justice for victims of cyber dependent crimes.

The nature of cyber dependent crimes varies with the type and target. The impact of a cyber crime tends to differ from one crime to other due to various factors like aim of the person, the target, demography and etc. When a closer understanding of the topic in respect of victims is carried out, it could be understood that the cyber dependent crimes influence the victims psychologically. It affects the behaviour and attitude of victims. Various victims of cyber dependent crimes show signs of anti social behavioural traits and traits of cynicism. It is a well founded principle that the goal of restorative justice is address the need of victims. However in the Indian jurisprudence, the restorative tool remains constant and the difference in the need of victims is unknown.

Certain countries focus on a need based approach while certain countries focus on a right based approach. It is quite interesting to find out that countries like the United States, where right based approach is followed, thus difference in the need of the victims is recognized and addressed. However in India, since need based approach is followed, the difference in the need of cyber dependent crime victims is unknown. If there is difference in the need of cyber dependent crime victims, a conclusion that the current system is a failure could be made and the swift of approach becomes mandatory. Thus this research aims in finding out difference in the need of cyber dependent crime victims

Review of Literature

Cyber-dependent crimes (or 'pure' cyber crimes) are offences that can only be committed using a computer, computer networks or other form of information communications technology (ICT). These acts include the spread of viruses or other malware, hacking and distributed denial of service (DDoS) attacks. Definitions of these are outlined below. They are activities primarily directed against computers or network resources, although there may be a variety of secondary outcomes from the attacks. For example, data gathered by hacking into an email account may subsequently be used to commit a fraud. This chapter refers only to cyber-dependent crimes in their primary form – as offences 'against' computers and networks.

Main forms of cyber-dependent crime

Cyber-dependent crimes fall broadly into two main categories:

• illicit intrusions into computer networks (for example, hacking); and

• the disruption or downgrading of computer functionality and network space

(for example, viruses and DDoS attacks).

Cyber-dependent crimes vary in the extent to which they target specific victims, or are more random in nature. Viruses, for example, may be widely spread to infect large numbers of victims indiscriminately. Advanced persistent threats (APTs), on the other hand, refer to highly planned, sophisticated and prolonged attacks to achieve a specific goal, for example, in terms of taking

down infrastructure or obtaining specific information about a person or organisation (Symantec, 2012).

Victimisation in cyber dependent crimes

Most surveys of the general public and businesses capture information on internet users' negative online experiences. The most robust of these, and conducted on a regular basis, are the Crime Survey for England and Wales, and surveys by the Oxford Internet Institute. One-off surveys have also been conducted by the ONS (2010) and Ipsos MORI (2013). Amongst businesses, one of the most robust surveys available is the 2012 Commercial Victimisation Survey (CVS).

These surveys do not, however, measure criminal activity or police recorded crime. So whilst they can be useful indicators, they do not give firm measures of prevalence for cyber-dependent (or cyber-enabled) crimes. It is unlikely that many of the experiences recorded in these surveys would meet the specific criteria to be classified as a 'crime' under Home Office Counting Rules.

NCC (2012) also reported that hacking activity originating from the UK appeared to decrease during 2012. In the 1st quarter of 2012 the UK was ranked 7th in the world for hacking activity (representing 2.4% of all attacks globally), falling to 12th by the 3rd quarter (representing 1.6% of all attacks). The US remained the number one country for the origin of hacks in the 3rd quarter of 2012, representing nearly 21 per cent of all attacks globally, followed by Russia (19.1%) and China (16.3%).

Classifying Trends of victimisation

Around one-third (37%) of adult internet users in the CSEW 2011/12 reported one or more 'negative online experiences' in the year prior to being interviewed This was a small, but statistically significant decrease from 39 per cent in 2010/11 occurring largely as a result of a statistically significant decrease in the proportion of users experiencing a computer virus. Similarly, Ipsos MORI (2013) found that 36 per cent of adult internet users had experienced one or more negative incidents online in the year to March 2012.

Viruses are one of the most common negative online experiences reported (for example, in the CSEW; Oxford Internet Survey; Ipsos MORI). According to the 2011/12 CSEW, almost one-third

(31%) of adult internet users experienced a virus in the 12 months prior to interview. This compares with just three per cent reporting 'loss of money' in the same time period. Only receipt of spam has featured more highly in other surveys – reported by 54 per cent of internet users surveyed by ONS (2010) – though these surveys are not directly comparable.

The proportion of adult internet users experiencing computer viruses appears to have decreased since the mid-2000s. Earlier data from the CSEW (formerly known as the British Crime Survey, see Figure 1.1) shows that the proportion of adult internet users experiencing computer viruses fell from a high point in 2005/06 (41%), to 31 per cent in 2011/12 However, it should be noted that the wording of the question changed during this time period so the figures are not directly comparable and also the survey questions were not asked every year. The Oxford Internet Survey presents a slightly different trend, showing an increase in virus experiences from 31 per cent in 2009 to 38 per cent in 2011, followed by a fall in 2013 to 30 per cent.

Research methodology

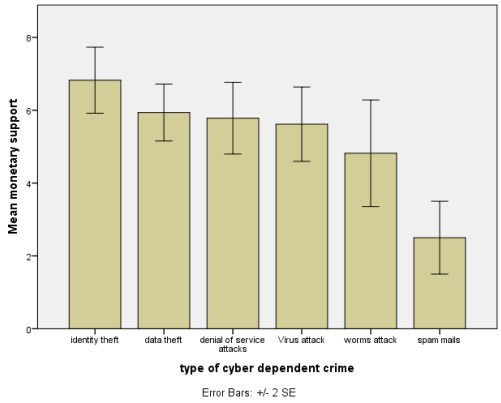
This socio-legal, empirical study is carried out to identify the psycho emotional impact of self isolation through lockdown on the behaviour of individuals from organised sector

This research is carried out by determining the level of each narcissistic trait among the respondents using different social media networking sites. The study includes both qualitative as well as quantitative methods. Since analyzing the level of each trait is required the study also includes an analytic method. Present study is based on Primary as well as Secondary sources of data, which are as Primary Sources collected by interview from victims and Secondary Sources collected through literature of N.G.O. reports, Government Reports, Websites, Research Articles, Newspapers. The study is dependent on Independent variables like age and and Dependent variable.

The study is carried out with the help of a convenient sampling method, having 253 sample size from an open sample frame. The statistical tools used for the purpose of deriving results are graphs, pie charts, Pearson correlation, Mann Whitney U test, independent t test and Kendall's tau_b test.

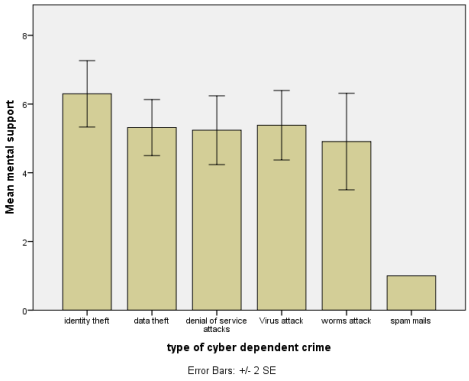
Graphs and Analysis

Graph1. The Bar Graph depicting the difference in need of monetary support in various types of cyber dependent crimes



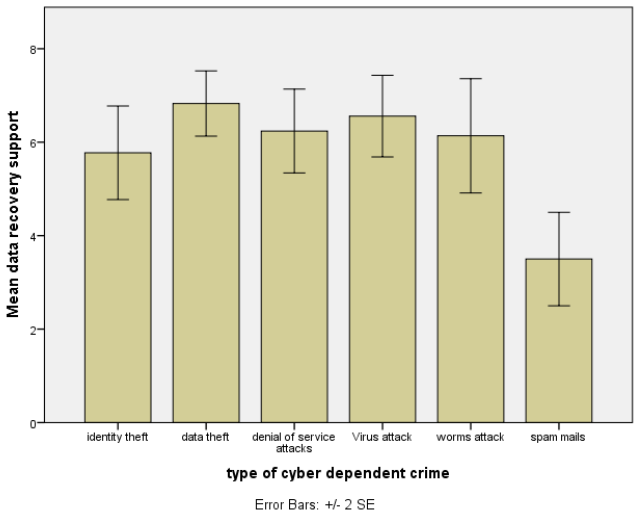
This graph depicts the contrasting levels in need of monetary support among victims of cyber dependent crimes

Graph2. The Bar Graph depicting the difference in need of mental support in various types of cyber dependent crimes



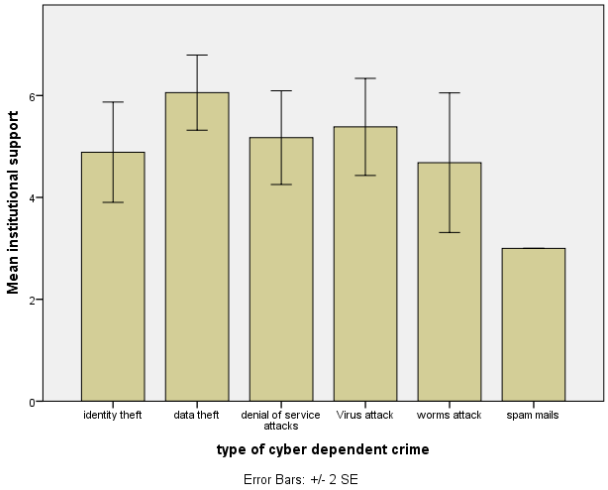
This graph depicts the contrasting levels in need of mental support among victims of cyber dependent crimes

Graph3. The Bar Graph depicting the difference in need of data recovery support in various types of cyber dependent crimes



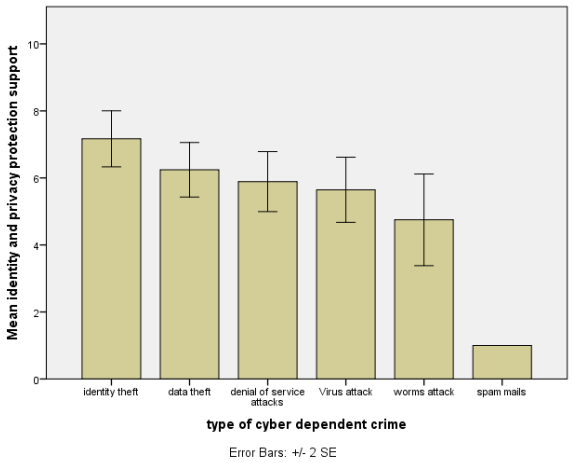
This graph depicts the contrasting levels in need of data recovery support among victims of cyber dependent crimes

Graph4. The Bar Graph depicting the difference in need of institutional support in various types of cyber dependent crimes



This graph depicts the contrasting levels in need of **institutional support** among victims of cyber dependent crimes

Graph5. The Bar Graph depicting the difference in need of identity and privacy protection support in various types of cyber dependent crimes



This graph depicts the contrasting levels in need of **identity and privacy protection support** among victims of cyber dependent crimes

Analysis1. Mann Whitney U test

	monetary support	mental support	data recovery support	institutional support
Mann-Whitney U	7544.000	7508.000	7676.000	7446.000
Wilcoxon W	18719.000	18683.000	18851.000	18621.000
Z	-.360	-.427	-.128	-.535
Asymp. Sig. (2-tailed)	.719	.670	.898	.592

This non parametric test is done between scale and a nominal variable containing 2 definite samples

Analysis 2. Kruskal Wallis Test

	monetary support	mental support	data recovery support	institutional support

Chi-Square	15.389	7.665	5.615	9.844
Df	4	4	4	4
Asymp. Sig.	.004	.105	.230	.043

This non parametric test is done between scale and a nominal variable containing ‘n’ definite samples

Analysis 3. One-Sample Test, lower limit difference

	Test Value = 0				
	T	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference
					Lower
identity and privacy protection support	28.248	252	.000	6.008	5.59

Analysis 4. One-Sample Test, upper limit difference

	Test Value = 0
	95% Confidence Interval of the Difference
	Upper

identity and privacy protection support	6.43

Results

From graph 1 it could be identified that the level of monetary support requirement/ need is high among of the victims of identity theft. The level of monetary support requirement/ is low in the victims of spam mails. Based on the intensity of the offence the level of monetary support requirement/ varies. Level of monetary support requirement/ reduces as the intensity of offence reduces.

From graph 2 it could be identified that the levels in need of mental support is high among of the victims of identity theft. The levesl in need of mental support is low in the victims of spam mails. Based on the intensity of the offence the level in need of mental support varies. Level in need of mental support reduces as the intensity of offence reduces. However in the case of virus attack the level of irritability is comparatively high.

From graph 3 it could be identified that the level in need of data recovery support is high among of the victims of data and virus attack. The level of hostility is low in the victims of spam mails. Based on the intensity of the offence the level of hostility varies. Level of hostility reduces as the intensity of offence reduces.

From graph 4 it could be identified that the level of hyper vigilance is high among of the victims of identity theft. The level of hyper vigilance is low in the victims of spam mails. Based on the intensity of the offence the level of hyper vigilance varies. Level of hostility reduces as the intensity of offence reduces.

From graph 5 it could be identified that the level of post traumatic stress disorder is high among of the victims of identity theft. The level of post traumatic stress disorder is low in the victims of spam mails. Based on the intensity of the offence the level of post traumatic stress disorder varies. Level of post traumatic stress disorder reduces as the intensity of offence reduces.

Analysis 1 depict that need(supports) is the same between male and females. However in a very few cases in female is more prevalent in than males.

Analysis 2 depict that need requirements varies across different age groups. The prevalence of post traumatic stress disorder is high in the age group 18-28 and the age group that includes individual in age of 62 years and above.

Analysis 3 depict that prevalence of social isolative behaviour varies across different age groups. The prevalence of social isolative behaviour is high in the age group 18-28 and the age group that includes individual in age of 62 years and above.

Discussions

The level of agitation is high among of the victims of identity theft. The level of agitation is low in the victims of spam mails. Based on the intensity of the offence the level of agitation varies. This variation is due to the degree of intensity of the offence. Level of agitation reduces as the intensity of offence reduces. This principle applies in the case of other behavioural characteristics also.

in the case of virus attack the level of irritability is comparatively high, which breaks the principle established above due to the impact of the virus attack due to the effect of virus attack in the computer. Generally a virus would affect the functioning of the computer thus the irritability levels stay high.

Though the prevalence of post traumatic stress disorder is the same between male and females, in a very few cases post traumatic stress disorder in females is more prevalent than males because the level of sensitivity in females is high compared to male, Thus the result.

The prevalence of post traumatic stress disorder is high in the age group 18-28 and the age group that includes individuals aged 62 years and above is because of the trait spectrum influence on age.

Conclusion

From the current study it could be identified that it could be identified that the level of monetary support requirement/ need is high among of the victims of identity theft. The level of monetary

support requirement/ is low in the victims of spam mails. Based on the intensity of the offence the level of monetary support requirement/ varies. Level of monetary support requirement/ reduces as the intensity of offence reduces. This difference could be traced in other forms of needs as well. The study is able to find out that need requirements varies across different age groups. The data protection and privacy support requirment is high in the age group 18-28 and the age group that includes individual in age of 62 years and above. It also depict that prevalence of social isolative behaviour varies across different age groups. The restorative support is high in the age group 18-28 and the age group that includes individual in age of 62 years and above. These finding permits to make a conclusion that there is difference in the need of cyber dependent crime victims, and the current system is a failure, the swift of approach becomes mandatory.