ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Enough Law of Horses and Elephants Debated…… …….Let's Discuss the Cyber Law Seriously

Sandeep Mittal (IPS)
Director
LNJN National Institute of Criminology & Forensic Science
Ministry of Home Affairs, New Delhi, India

Prof. Priyanka Sharma
Professor & Head
Information Technology & Telecommunication,
Raksha Shakti University, Ahmedabad, India

Abstract: The unique characteristic of cyberspace like anonymity in space and time, absence of geographical borders, capability to throw surprises with rapidity and potential to compromise assets in virtual and real world has attracted the attention of criminal minds to commit crimes in cyberspace. The law of crimes in the physical world faces challenge in its application to the crimes in cyberspace due to issues of sovereignty, jurisdiction, trans-national investigation and extra-territorial evidence. In this paper an attempt has been made to apply routine activity theory (RAT) of crime in physical world to crime scene cyberspace. A model for crime in cyberspace has been developed and it has been argued that the criminal law of crime in physical world is inadequate in its application to crimes in virtual world. To handle crime in cyberspace there is a need to address issues of 'applicable laws and 'conflicting jurisdiction by regulating the architecture of the internet through special laws of cyberspace. A case has been put forward for having an International Convention of Cybercrime with Council of Europe Convention on Cybercrime as yard stick.

Keywords: Cybercrime; Cyber Law; Cyberspace; Routine Activity Theory (RAT); Cyber-criminology; EU Convention on Cybercrime; Law of Horse

I. INTRODUCTION

The 'Internet' has today become an essential part of our lives and revolutionised the way communication and trade take place far beyond the ambit of national and international borders. It has, however, also allowed unscrupulous criminals to misuse the Internet and exploit it for committing numerous cybercrimes pertaining to pornography, gambling, lottery, financial frauds, identity thefts, drug trafficking, and data theft, among others [1]. Cyberspace is under both perceived and real threat from various state and non-state actors [2] [3] [4]. The incidence of cyber-attacks on information technology assets symbolises a thin line between cybercrime and cyber war, both of which have devastating outcomes in the physical world [5] [6]. The scenario is further complicated by the very nature of cyber space, manifested in its anonymity in both space and time, and asymmetric results that are disproportionate to the resources deployed, and the fact that the absence of international borders in cyber space makes it impossible to attribute the crime to a tangible source [7]. In the context of these characteristics of cyberspace, 'the transnational dimension of cybercrime offence arises where an element or substantial effect of the offence or where part of the modus operandi of the offence is in another territory', bringing forth the issues of 'sovereignty, jurisdiction, transnational investigations and extraterritorial evidence'; thus necessitating international cooperation [8]. The evolution of cybercrimes from being simple acts perpetrated by immature youngsters to complex cyber-attack vectors through the deployment of advanced technology in cyberspace has necessitated the development of a distinct branch of Law, The Law of Cyberspace. However, the question of whether 'the law of cyberspace' can evolve into an independent field of study or would remain just an extension of the criminal laws of the physical world in the virtual world has become the subject of an interesting debate among legal and social science scholars. The scope of this essay is to critically analyse and compare traditional crimes with cybercrimes to assess if a new set of laws is required for tackling crimes in cyberspace or otherwise.

II. THE CYBER-ZOO: THE ELEPHANT VERSUS THE HORSE AS SYMBOLS OF CYBERSPACE REALITIES

In his poem, 'The Blind Men and the Elephant', John Godfrey Saxe describes the dilemma of six blind men while trying to describe the elephant (which) "in (this) sense represents reality, and each of the worthy blind sages represents a different approach to understanding this reality. In all objectivity, and in line with the poem of John Godfrey Saxe, all the sages (blind men) have correctly described their piece of reality, but fail by arguing that their reality is the only truth." [9] To quote,

"And so these men of Indostan,
Disputed loud and long,
Each in his own opinion,
Exceeding stiff and strong,
Though each was partly in the right,
And all were in the wrong!"[10]

In the context of this article, cyberspace can be compared with the elephant, which is understood and described differently by different stakeholders in the realms of sociology, criminology, law, technology, and commerce, among other disciplines. However, each of the stakeholder largely ignores the perspective of the others while also understating or overstating the complexity inherent in the physical and virtual processes manifested through the interplay of 'technology with technology' and 'technology with humans' in virtual space, which, in turn, is not constrained by the barriers of geography, culture, ethnicity and sovereignty of state, but still has manifestation in the physical world. A few legal scholars have also explored the concept of the cyber elephant for determining the principles needed to regulate cyberspace [11].

In 1996, Judge Frank Easterbrook delivered a lecture [12] at the University of Chicago where he discussed his ideas on ‘property in cyberspace’. He explained that coalescing two fields, without knowing much about either, in the name of ‘cross-sterilisation of ideas’ is putting [lawyers] at the ‘risk of multi-disciplinary dilettantism’. He argued that there are a large number of cases relating to various aspects of dealing with horses such as the sales of horses, people being kicked by horses, theft of horses, racing of horses or medical care of horses, but this alone cannot be the reason for designing a course on “The Law of Horses”, as that would signify shallow efforts towards understanding the unifying principles of such a law [13]. This led to the current debate on the need for a separate law of cyberspace [14]. However, scholars have strongly challenged the position taken by Judge Easterbook [15] [16] [17].

III. TRADITIONAL CRIMES IN THE REAL WORLD VERSUS CYBERCRIMES

Acquiring a deep understanding of the theories of traditional crime in the physical world and their application to crimes in cyberspace would help us in identifying the factors that might govern the regulation of cyberspace. The basic components of acts of crime in the real world and how they intrinsically differ from crimes in cyberspace have been discussed and summarised in Table 1 [18]. Brenner concludes that “cybercrime differs in several fundamental respects from real-world crime and the traditional model is not an effective means of dealing with cybercrimes” [19] and that the “matrices for the real world crime do not apply to cybercrime, as it differs in the methods that are used in its commission and in the nature and extent of the harms it produces” [20]. Interestingly, Brenner had earlier adopted a more conservative stand on the law applying to cybercrime [21].

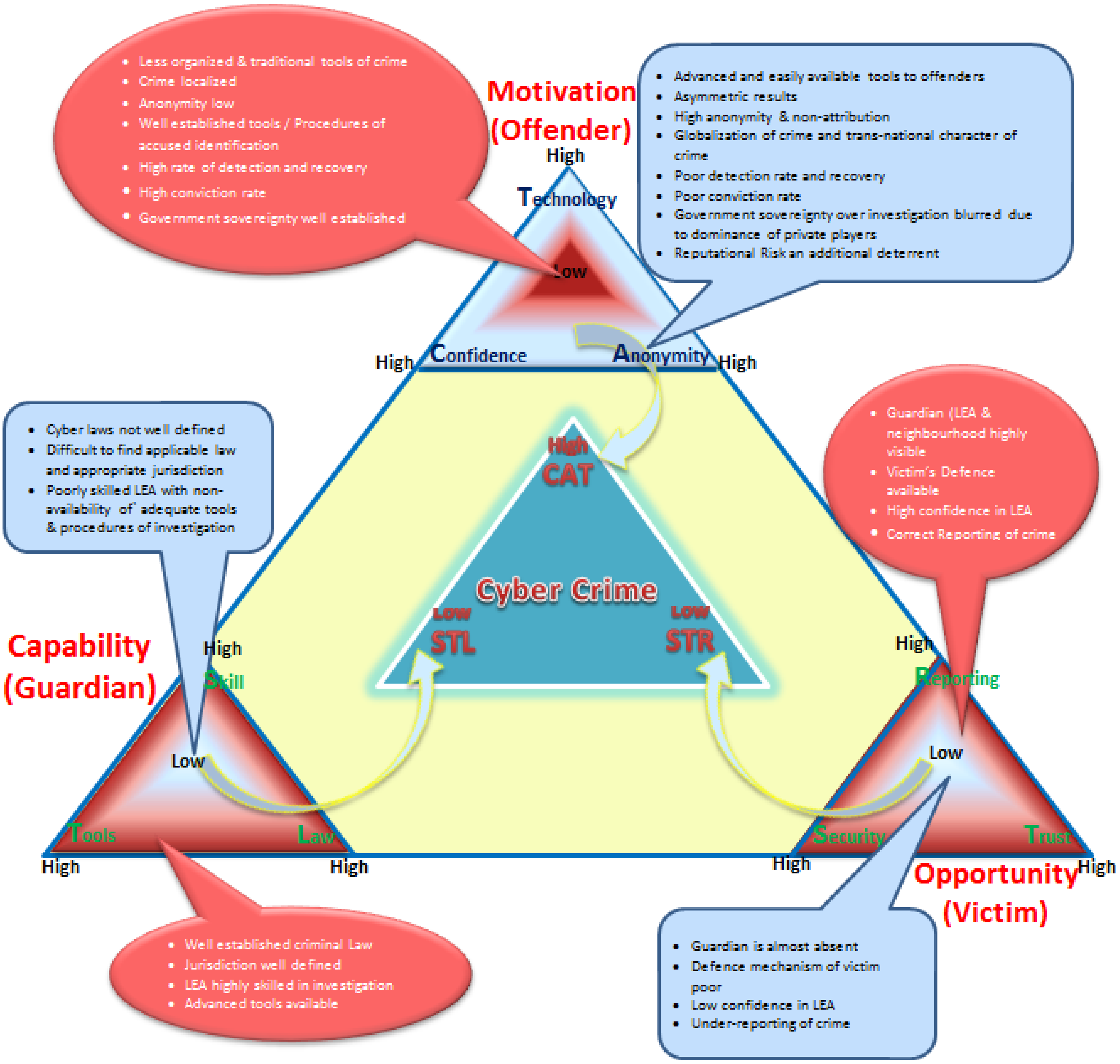
Theories of criminology have been applied to cyberspace to explore its interaction with the human dimension, as perceived by criminologists (potential dilettante) [23] [24]. The Routine Activity Theory (RAT) relating to crime in the real world has been studied by scholars to analyse if it can be transposed to cybercrime or otherwise [25]. RAT assumes that the minimum three factors required for a crime are an ‘opportunity’ in the form of a suitable target (victim), a ‘motivated offender’ with criminal inclination, and the ‘absence of a capable guardian’ (a law enforcement agency, the neighborhood, etc.). Lack of any one of these factors would prevent the occurrence of the crime [26] [27]. The different controls in traditional crimes and cybercrimes seen in the context of RAT have been depicted in Figure 1 [28] [29] [30].

The three constituents of RAT, viz. the Victim, Offender and Guardian, have been represented by the three vertices of the largest triangle. Each of these three controls is further dependent on sub-factors, which, in turn, are represented as three triangles (for each of these sub-factors, a low value is assigned to the Centre and a high value to the vertex) placed respectively, at each of the vertices of the main triangle. The distinction between traditional crime (Red) and cybercrime (Blue) due to the complex interplay of multiple factors is obvious. Last but not the least, the blue triangle in the Centre characterises cybercrime. The basic tenets of RAT thus fit in well with the paradigm of cybercrimes.

Table 1: Traditional Crimes versus Cybercrimes [22]

1.	Proximity—the perpetrator and the victim are physically proximate at the time of committing of the crime.	No physical proximity is required between the offender and the victim.
2.	The crime is a ‘**one-to-one**’ event involving the perpetrator(s) and victim(s).	A perpetrator can automate the process of victimisation and commit thousands of cybercrimes with high speed at the same time.
3	The committing of the crime is subject to ‘**physical constraints**’ governing all activities in the physical world.	Real-world constraints do not affect perpetrators of cybercrimes, as they can be committed with anonymity, at lightning speed, and traverse beyond transnational borders.
4.	The demographic contours and geographical patterns of the incidence of crime are identifiable.	It is difficult to identify the patterns and contours of cybercrime due to the lack of uniformity in the definition of cybercrimes, absence of laws, technologies evolving at a faster pace, the anonymity that the perpetrator of the cybercrime enjoys in space and time, and the under-reporting of cybercrimes due to the fact that it poses a risk to many reputations.

It has been argued that the routine activity approach has both significant continuities and discontinuities in the configuration of terrestrial and virtual crimes. “While motivated offenders are likely to be almost homogeneous in both environments, the construction of suitable targets is complex, with similarity on value scale but significantly different in respect of inertia, visibility and accessibility.” [31] The concept of the ‘capable guardian’ fits in well in both settings but the degree of fitness varies. However, the spatio-temporal environment of routine activities is organised in the real world but organically disorganised in the virtual world [32]. Thus, these features of cyberspace make it a domain-distinct from the real world,[33] resulting in noticeably low level of reporting of cybercrimes as compared to that of traditional crimes, as depicted in Figure 2 [34].



- Less organized & traditional tools of crime
- Crime localized
- Anonymity low
- Well established tools / Procedures of accused identification
- High rate of detection and recovery
- High conviction rate
- Government sovereignty well established

- Advanced and easily available tools to offenders
- Asymmetric results
- High anonymity & non-attribution
- Globalization of crime and trans-national character of crime
- Poor detection rate and recovery
- Poor conviction rate
- Government sovereignty over investigation blurred due to dominance of private players
- Reputational Risk an additional deterrent

- Cyber laws not well defined
- Difficult to find applicable law and appropriate jurisdiction
- Poorly skilled LEA with non-availability of adequate tools & procedures of investigation

- Guardian (LEA & neighbourhood highly visible
- Victim's Defence available
- High confidence in LEA
- Correct Reporting of crime

- Well established criminal Law
- Jurisdiction well defined
- LEA highly skilled in investigation
- Advanced tools available

- Guardian is almost absent
- Defence mechanism of victim poor
- Low confidence in LEA
- Under-reporting of crime

Figure 1: RAT and Interplay of Different Controls in Traditional Versus Cyber Crimes

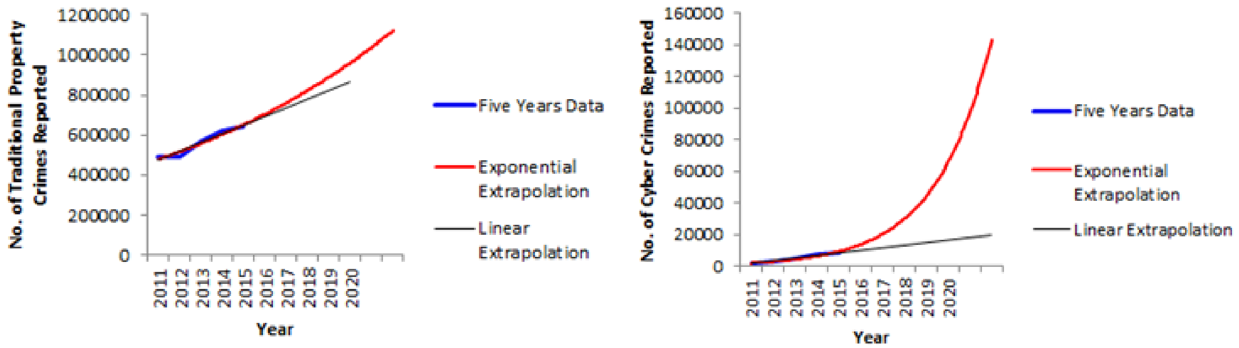


Figure 2: A Comparison of Traditional Property Crimes versus Cybercrimes over a Period of Five Years in India (Source of Statistics: Crime in India Statistics, NCRB)

Thus, the various factors that incite an individual to commit a cybercrime include the lack of deterrents, increased anonymity, and repressed desires to offend in the real world [35]. While the issue of repressed desires can be handled in traditional ways, the other two issues need to be handled through regulation of both the law and technology, or one of the two facilitating regulation of the other. The absence of any perimeter in cyberspace also makes it easily permeable, thereby making it difficult to assign an appropriate capable guardian for overseeing activities in cyberspace [36].

Thus an individual commit cybercrime due to the lack of deterrents, Some economists have averred that people are actively involved in "transforming their relationships into social capital and their experiences into human capital (conventional or criminal)" and that these economic considerations are more compelling than the criminologist's simple theory that a crime occurs in response to 'associations' and 'events' [37]. In fact, altering the criminal's economic choice pattern may also help alter his behavior [38] [39]. The model of cybercrime portrayed in Figure 1 does not contradict this contention.

IV. MOVING FROM THE 'DILETTANTISM' OF CYBER-CRIMINOLOGY TO THE LAW OF CYBERSPACE

After analysing and understanding the various factors that contribute to the commission of a crime in cyberspace, it may be suggested that any law enacted to regulate cyberspace would have to address the following three unique features of cyberspace [40]:

(a) As 'computer-assisted' low-cost efforts produce asymmetric results disproportionate to the resources deployed, the law should thus develop mechanisms for increasing the cost entailed in the crime and decrease the probability of its success. For example, there should be a thorough investigation of the crimes wherein victims implemented security measures to make their systems fool proof and exercised due diligence, whereas an enhanced-sentencing regime should be employed where dual-use technology like encryption techniques or anonymity has been used to commit the crime.

(b) There is a need to add third parties (such as Internet Service Providers or ISPs) to the traditional 'offender-victim' scenario of the crime. The law could consider imposing responsibilities on these third parties though it may be difficult to implement in view of the costs and liabilities implied in such actions. For example, in the United States, the Digital Millennium Copyright Act (DMCA) specifies the liability of 'online-intermediaries' in case of intellectual property right violations but no liability of 'online-intermediaries' is provided for defamation under The Communications Decency Act (CDA).

(c) The invisibility of the action in cyberspace and anonymity of the offender limit the capability of the guardian to regulate. It is possible for the law to address this issue. For example, the law may make implementation of IPV06 mandatory for the more specific attribution of acts in cyberspace or the law may mandate a change in the Internet architecture to include controls that would help in the identification of the perpetrators. As most of the Internet architecture is designed, maintained, controlled and governed by private bodies, the law would have to factor in the responsibilities and liabilities of these private stakeholders through either state regulation or self-regulation. Another example would be to make the use of digital signatures (using PKI) mandatory for communication in cyberspace, which in itself would not only prevent the occurrence of many crimes but also assist in the detection of crimes that still manage to be perpetrated despite the imposition of stringent checks.

Therefore, technology-intensive cybercrimes compel us to revisit the role and limitations of criminal law, just as criminal law forces us to reinvent the role and limitations of technology [41]. However, there is a symbiotic relationship between the two.

The adage, "On the Internet, nobody knows that you're a dog" [42] is as true today as it has been throughout the history of the Internet, but the problem plaguing law enforcement agencies today is that, "on the Internet, nobody knows where the dog is" [43]. This is because the functionality of the Internet and its architecture are technologically indifferent to geographical location [44], leaving no scope for coherence in real space and cyberspace, wherein the latter is characterised by 'geographical indeterminacy' [45]. This gives rise to the legal issue of 'appropriate jurisdiction' or even 'conflicting jurisdiction' for cybercrimes. Criminal law is territorial in its applicability, and as territory itself is indeterminate in cyberspace, the applicable law and the appropriate jurisdiction would need to be determined in accordance with the principles of private international law, as is being done in the resolution of e-commerce disputes. But, do the principles of the civil liability transpose well into the realm of criminal liability? Although this is procedurally possible, the answer would still be substantively 'no', particularly when the definition of cybercrime itself may not be known in many jurisdictions. These legal issues need to be addressed for detection, investigation, prosecution and conviction of the criminals in cyberspace. And international cooperation is imperative in order to find where the 'dog' is, as it involves issues of sovereignty, jurisdiction, transnational investigations and examination of extraterritorial evidence.

V. THE CODE: THE INTERNET DOG, TECHNOLOGY, THE LAW, AND THE INTERNET GOD

Lawrence Lessig, in his theoretical model of cyberspace regulation [46], argued that behaviour is regulated by four constraints, viz., laws, social norms, markets, and nature [47]. The law, however, indirectly regulates behaviour while directly influencing the other three constraints, namely, social norms, markets, and nature. Applying this concept to cyberspace, Lessig postulated that in cyberspace, the equivalent of 'nature' is 'code' [48], with the latter being a more pervasive and effective constraint in cyberspace. The code is also more susceptible to being changed by law than the nature. Therefore, both the 'code' and 'law' have the potential of regulating the behaviour in cyberspace [49]. It has been argued that regulation in cyberspace would be more efficient and effective if the law regulates code rather than individual behavior [50].

The 'code' being expounded by Lessig was meant to include merely the software. With the advent of advanced technology in cyberspace, however, it is obvious that code would have to include not only the software, but also the concomitant hardware, Internet protocols, standards, biometrics, and privately controlled governance structures. All these components collectively contribute to the character and peculiarities of the Internet, making it the way it is. The code could then be safely given a new name, viz., 'cyberspace architecture' [51], with every component of this architecture having the potential of being regulated by law.

However, as pointed out earlier, even if various national Governments have enacted some type of law pertaining to cybercrimes, inconsistencies and disharmony remain in their application in transnational environments as criminal law is territorial. This necessitates international cooperation in either an informal or formal manner. Further, evidence gathered through the former is not admissible in courts, while evidence gathered through the latter is delayed due to the prevalence of long-drawn procedures, resulting in the escape of the 'dog'. The solution could thus lie in the creation of an 'International Framework on Cybercrime' for addressing various legal issues relating to cyberspace.

The Council of Europe Convention on Cybercrime (the Convention) [52] is the first comprehensive framework on cybercrime which puts forth 'instruments to improve international cooperation' [53] and 'duly takes into account the specific requirements of the fight against cybercrime' [54]. The Convention has the potential of becoming an International Cyber Law like the Private International Law that has evolved over a period of time, but would have to be used in harmony with the substantive criminal law of the territory. The complex interaction between the two underscores the necessity for the enactment a separate set of laws to handle cybercrime.

VI. CONCLUSION

Cyberspace is increasingly becoming a favourite domain for criminals for not only committing crimes but also for maintaining secret global criminal networks. This is because the organic nature of cyberspace is manifested in anonymity in space and time, immediacy of effects, non-attribution of action, and the absence of any international borders. Due to the unique nature of cyberspace, it is difficult to apply the laws of criminal liability for traditional crimes to cybercrimes. An examination of the traditional theories reveals that cybercrime is fundamentally different from crimes in the real world, and the traditional models are not effective in dealing with cybercrime. However, the dynamics of cybercrime was explained by transposing the factors operating in Routine Activity Theory (RAT) to cyberspace. It was demonstrated that the higher levels of anonymity, confidence and technological skills enjoyed by the offender motivate him to choose and target a victim who has been rendered vulnerable by the prevalent low level of security, trust and crime-reporting emanating from poorly defined laws, poor technical skills, and deficit of trust in the law enforcement machinery. The detection, investigation, prosecution, and successful conviction of the perpetrator of a cybercrime require the law to address the specific features of crime in virtual space. Anonymity and invisibility of action in cyberspace and its 'geographic indeterminacy' give rise to the legal issues of 'applicable laws' and 'conflicting jurisdiction'. The architecture of the Internet needs to be governed by law, which has the potential to improve the behaviour of criminals in cyberspace. This would also entail international cooperation to address the issues of sovereignty, jurisdiction, transnational investigations, and extraterritorial evidence. It is suggested that the Council of Europe Convention on Cybercrime could be a yardstick for initiating measures in this direction. However, all this does not preclude the need for a separate set of laws for handling cybercrimes and providing legal remedies against them.

VII. REFERENCES

[1] Sandeep Mittal, 'A Strategic Road-map for Prevention of Drug Trafficking through Internet' (2012) 33 Indian Journal of Criminology and Criminalistics 86

[2] Marco Gercke, Europe's legal approaches to cybercrime (Springer 2009)

[3] Marco Gercke, 'Understanding cybercrime: a guide for developing countries' (2011) 89 International Telecommunication Union (Draft) 93

[4] David L Speer, 'Redefining borders: The challenges of cybercrime' (2000) 34 Crime, law and social change 259

[5] Sandeep Mittal, 'Perspectives in Cyber Security, the future of cyber malware' (2013) 41 The Indian Journal of Criminology 18

[6] Sandeep Mittal, 'The Issues in Cyber- Defense and Cyber Forensics of the SCADA Systems' (2015) 62 Indian Police Journal 29

[7] Sandeep Mittal, 'A Strategic Road-map for Prevention of Drug Trafficking through Internet'

[8] Open-ended Intergovernmental Expert Group on Cybercrime, Comprehensive Study on Cyber Crime, 2013)

[9] https://wildequus.org/2014/05/07/sufi-story-blind-men-elephant/ (Accessed on 13/04/2017)

[10] http://www.constitution.org/col/blind_men.htm (Accessed on 13/04/2017)

[11] Martina Gillen, 'Lawyers and cyberspace: Seeing the elephant' (2012) 9 ScriptED 130

[12] Frank H Easterbrook, 'Cyberspace and the Law of the Horse' (1996) U Chi Legal F 207

[13] Ibid at 207, para 3

[14] Joseph H Sommer, 'Against cyberlaw' (2000) Berkeley Technology Law Journal 1145

[15] Lawrence Lessig, 'The law of the horse: What cyberlaw might teach' (1999) 113 Harvard law review 501

[16] Andrew Murray, 'Looking back at the law of the horse: Why cyberlaw and the rule of law are important' (2013) 10 SCRIPTed 310

[17] James Baxendale, 'FORTIETH ANNIVERSARY ISSUE: EQUINE CONSIDERATIONS AND COMPUTER LAW-REFLECTIONS FORTY YEARS ON' (2010) 36 Rutgers Computer & Tech LJ 161

[18] Susan W Brenner, 'Toward a criminal law for cyberspace: A new model of law enforcement' (2004) 30 Rutgers Computer & Tech LJ 1

[19] Ibid at page 104

[20] Susan W Brenner, 'Cybercrime Metrics: Old Wine, New Bottles?' (2004) 9 Va JL & Tech 13

[21] Susan W Brenner, 'Is There Such a Thing as' Virtual Crime'?' (2001)

[22] Brenner, 'Toward a criminal law for cyberspace: A new model of law enforcement'

[23] Miltiadis Kandias and others, An insider threat prediction model (Springer 2010)

[24] Sandeep Mittal, 'Understanding the Human Dimension of Cyber Security' (2015) 34 Indian Journal of Criminology and Criminalistics 141

[25] Majid Yar, 'The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory' (2005) 2 European Journal of Criminology 407

[26] Ibid

[27] Lawrence E Cohen and Marcus Felson, 'Social change and crime rate trends: A routine activity approach' (1979) American sociological review 588

[28] Nir Kshetri, 'The simple economics of cybercrimes' (2006) 4 IEEE Security & Privacy 33

[29] Yar, 'The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory'

[30] Majid Yar, Cybercrime and society (Sage 2013)

[31] Yar, 'The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory'. at page424

[32] Ibid

[33] Mittal, 'A Strategic Road-map for Prevention of Drug Trafficking through Internet'

[34] Statistics Source: Crime in India Statistics, NCRB, Ministry of Home Affairs, Government of India, New Delhi.

[35] Karuppannan Jaishankar, 'Establishing a theory of cyber crimes' (2007) 1 International Journal of Cyber Criminology 7

[36] Susan W Brenner, 'Toward a criminal law for cyberspace: Product liability and other issues' (2004) 5 Pitt J Tech L & Pol'y i

[37] Bill McCarthy, 'New economics of sociological criminology' (2002) 28 Annual Review of Sociology 417

[38] JR Probasco and William L Davis, 'A human capital perspective on criminal careers' (1995) 11 Journal of Applied Business Research 58

[39] Kshetri, 'The simple economics of cybercrimes'

[40] Neal Kumar Katyal, 'Criminal law in cyberspace' (2001) 149 University of Pennsylvania Law Review 1003

[41] Ibid

[42] https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html?utm_term=.8cc4b79354f7

[43] Alexandre López Borrull and Charles Oppenheim, 'Legal aspects of the Web' (2004) 38 Annual review of information science and technology 483

[44] Though every computer or smart device has a machine address which can be easily spoofed, we are talking here specifically about geographical location. The remote access, incognito logins, encrypted platforms for communication, anonymous remailers and availability of ‘cached’ copies of frequently accessed internet resources further complicate and make impossible to attribute actions in cyberspace.

[45] Dan L Burk, 'Jurisdiction in a World without Borders' (1997) 1 Va JL & Tech 1

[46] Lessig, 'The law of the horse: What cyberlaw might teach'

[47] In real space nature is represented by architecture.

[48] That includes software that makes internet to behave as it is.

[49] Graham Greenleaf, 'An endnote on regulating cyberspace: architecture vs law?' (1998)

[50] Lessig, 'The law of the horse: What cyberlaw might teach'

[51] Greenleaf, 'An endnote on regulating cyberspace: architecture vs law?'

[52] Council of Europe, Convention on Cybercrime, 23 November 2001, available at: http://www.refworld.org/docid/47fdfb202.html [accessed 26 February 2017]

[53] Ibid. Articles 23-35

[54] Ibid. Preamble