International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 06, June 2017
www.ijates.com
ijates
ISSN 2348 - 7550

CYBER CRIME: PERSPECTIVE OF INDIAN VS EUROPE CYBER CRIME

M.Mohankumar[1],S.Venkatesan[2],V.Malarvzhi[3]

[1]Assistant Professor, [2,3]M.Sc. Computer Science

Department of Computer Science, Karpagam University, (India)

ABSTRACT

Each crime has its effect particularly on society, country, and the world to the immense degree. By th observation of cybercrime and its wonder, it is uncovered that like previous violations it has severely influenced social existence of people. To comprehend the impact of cybercrime, it is important to consider the effect of two things PC innovation and Web on individuals as cybercrime is most likely starting out of these. This article depicts the distinctions of the Indian point of view and Europe viewpoint in Digital Crimes.

Keywords: Cyber Crime, ITA-Information Technology Act, ITAA-IT Amendment Act, IPC-Indian Penal Code, IEA-Indian Evidence Act, BBE-Bankers Book Evidence, COE-Council Of Europe, UNGGE-UN Group Of Government Experts.

I. INTRODUCTION

The historical backdrop of crime and crime restraint has been like the past of fighting: a crime is created, at that point a barrier counters the offense, at that point another offense counters the new protection. Assault rifles prompted the improvement of tanks which prompted the advancement of rocket-pushed explosives, and so forth. Digital crimes are all over the place, can transpire, whenever. A few cases of digital crime are recognizing burglary, putting away illicit data, PC infections, and misrepresentation. We will talk about every case in detail. Cybercrime is another kind of crime that happens in this Science and Technology years. There is a considerable measure of definitions for digital crime. Cybercrime is also known PC crime that alludes to any crime that includes a PC and a system. Cybercrime is characterized as crimes carried out on the web utilizing the PC as either a device or a focused-on casualty.Quick headways in data and correspondence innovation have formed a reasonable channel to huge assets of data for individuals. All things considered, with such points of interest, there would be instances of abuse for the wrong drive. Digital fear mongering is, and will without a doubt keep on being a steady issue for governments that must be taken care of mindfully for national security. Fear based oppression has gone up against another structure and it is at no time in the future constrained to attempting to simply make mass pulverization with the utilization of viciousness. The internet is the new skyline which is controlled by machine for data and correspondence among people over the world. In this way, crimes carried out in the internet are to be considered as digital violations. In a more extensive sense, digital crime is a crime on the web which incorporates digital stalking, betting, hacking, fear based oppression, extortion, digital burglary, explicit entertainment, streaming of infections and so on.

II. CYBER CRIMES: INDIAN PERSPECTIVE

The utilization of mobile internet and reliance of persons in each field, various different crimes identified with Computer and different contraptions in view of the web have advanced in the public. Such violations where the utilization of PCs coupled is included with the utilization of Internet are extensively named as Cyber Crimes. [1]. There was no law in India for representing Cyber crimes including protection issues, locale issues, licensed innovation rights issues and various other lawful inquiries. With the propensity of abusing of innovation, there emerged a requirement for strict statutory laws to control the criminal exercises in the digital world and to ensure the genuine feeling of innovation "Data **TECHNOLOGY ACT, 2000" [ITA 2000]** was instituted by Parliament of India to secure the field of internet business, e-administration, e- managing an account and additionally punishments and disciplines in the field of digital violations. The above Act was additionally altered as IT Amendment **Act, 2008 [ITAA-2008].** The **ITA-2000** characterizes "PC" implies any electronic attractive, optical, or other fast information handling gadget or framework which performs consistent, number juggling, and memory works by controls of electronic, attractive, or optical motivations, and incorporates all info, yield, preparing, capacity, PC software, or which are associated with correspondence offices or identified with the PC in a PC framework or PC arrange. "Computer" and 'PC framework' have been so broadly characterized and translated to mean any electronic gadget with information handling ability, performing PC capacities like legitimate, number juggling and memory capacities with info, stockpiling and yield capacities and in this manner, any top of the line programmable devices like even a clothes washer or switches and switches utilized as a part of a system can all be brought under the definition.

III. SCOPE AND OBJECTIVE

The degree and appropriateness of ITA- 2000 were expanded by its change in 2008. The word 'specialized gadgets' embedded having a comprehensive definition, taking into its scope mobile phones, PDA or such different gadgets used to transmit any content, recordings and so forth., like what was later being showcased as iPad or other comparative gadgets on Wi-Fi and cell models.[1]Though **ITA-2000** characterized 'computerized signature', be that as it may, said definition was unequipped for cooking needs an off hour and subsequently the term 'Electronic mark' was presented and characterized in the **ITAA - 2008** as a legitimately substantial method of executing marks. This incorporates advanced marks as one of the methods of marks and is far more extensive in ambit covering biometrics and other new types of making electronic marks not limiting the acknowledgment to computerized signature prepare alone. The new revision has supplanted Section 43 with Section 66. The Word **"hacking"** utilized as a part of Section 66 of prior Act has been evacuated and named as **"information burglary"** in this area and has additionally been augmented as **Sections 66A to 66F.** The segment covers the offenses, for example, the sending of hostile messages through correspondence benefit, deluding the beneficiary of the beginning of such messages, insincerely accepting stolen PCs or other specialized gadget, taking electronic mark or character, for example, utilizing another people's secret key or electronic signature, conning by personation through PC asset or a specialized gadget, openly distributing the data about any individual's area without earlier consent or assent, digital fear based oppression, the demonstrations of access to a PC asset without approval, such acts which can prompt any harm to any individual or result in harm or decimation of any property, while attempting to defile the PC through any infection like Trojan and so forth.

The offenses secured under segment 66 are cognizable and non-safeguard capable. While, the outcome of Section 43 of prior Act were Civil in nature having its cure as harms and pay just, however under Section 66 of the Amendment Act, if such act is finished with criminal expectation that implies ocean, at that point it will draw in criminal risk having cure in detainment or fine or both. Cybercrime implies unlawful act wherein the PC is utilized as a device or an objective or else both.

III. OBJECTIVES

- To take the overview of perspective in Indian and Europeans Countries.
- Examining cybercrimeperspective cybercrime scenario in India and Europe Countries.

IV. CYBER CRIMES: INDIAN PERSPECTIV

A. The (IPC)Indian Penal Code, 1860

The Indian Penal Code was changed by embedding "electronic" consequently treating the electronic records and reports on a standard with physical records and archives. [2].The Sections managing the false passage in a record or false report and so on (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 and so on.) have since been altered as 'electronic record and electronic archive' in this way bringing inside the ambit of IPC. Presently, electronic record and electronic reports have been dealt with quite recently like physical records and archives amid the commission of demonstrations of phony or distortion of physical records in a crime. After the above revision, the exploring organizations record the cases/charge- sheet citing the important areas of IPC under segment 463,464, 468 and 469 perused with the ITA/ITAA under Sections 43 and 66 in like offenses to ensure the proof as well as discipline can be secured and demonstrated under both of these or under both enactment.

B. The (IEA) Indian Evidence Act 1872

The previous organization of ITA, [3] all confirmation in a court were in the physical casing in a manner of speaking. After the nearness of ITA, the electronic records and reports were seen. The definition part of Indian Evidence Act was changed as "all documents including electronic records" were substituted. Diverse words e.g. 'propelled check', 'electronic edge', 'secure electronic record' "information" as used as a piece of the ITA, were in like manner installed to make them a player in the evidentiary importance under the Act. The key update was seen by affirmation of agreeableness of electronic records as confirmation as respected in Section 65B of the Act.

C.The Bankers' Books Evidence (BBE) Act 1891

Before going of ITA,[4] a bank should create the first record or other physical enlist or archive amid confirmation under the steady gaze of a Court. After institution of ITA, the definitions part of the BBE Act stood corrected as: "'financiers " books' incorporate records, day-books, cashbooks, account-books and every single other book utilized as a part of the standard business of a bank whether kept in the composed frame or as printouts of information put away in a floppy, circle, tape or whatever other type of electromagnetic information stockpiling gadget". At the point when the books comprise of printouts of information put away in a floppy, circle, tape and so on., a printout of such section ...confirmed as per the arrangements ....to the impact that it is a printout of such passage or a duplicate of such printout by the key bookkeeper or branch supervisor; and (b) an authentication by a man accountable for PC framework containing a concise portrayal of the PC framework and

the particulars of the protections received by the framework to guarantee that information is entered or whatever other operation performed just by approved people; the shields embraced to avoid and distinguish unapproved change of information ...to recover information that is lost because of systemic disappointment or The above correction in the arrangements in Bankers Books Evidence Act perceived the printout from a PC framework and other electronic archive as a legitimate report amid course of proof, gave, such print-out or electronic record is joined by a declaration in wording as said above.

D. Issues Not Covered Under ITA

ITA and ITAA, however, the point of interest initial step and turned into a breakthrough in the innovative development of the country; nonetheless, the current law is not sufficed. Many issues in Cybercrime and numerous crimes are still left revealed. [5] Territorial Jurisdiction is a noteworthy issue which is not palatable tended to in the ITA or ITAA. Ward has been specified in Sections 46, 48, 57 and 61 with regards to mediation prepared and the investigative system associated with and again in Section 80 and as a major aspect of the cops' forces to enter, scan an open place for a digital crime and so forth. Since digital crimes are fundamentally PC based violations and in this way, if the mail of somebody is hacked in one place by charged sitting far in another state, assurance of concerned P.S., who will take comprehension is troublesome. It is seen that the agents for the most part attempt to abstain from tolerating such dissensions on the grounds of the Ward. Since the cybercrime is geology freethinker, borderless, region free and for the most part spread over domains of a few wards; it is expected to legitimate preparing is to be given to every single concerned player in the field. Conservation of confirmation is additionally a major issue. Clearly while documenting cases under IT Act, all the time, opportunities to pulverize the essential effortlessly as proof may lie in some framework like the delegates' PCs or here and there in the adversary's PC framework as well. In any case, the greater part of the digital violations in the country are still brought under the important segments of IPC perused with the relative areas of ITA or the ITAA which gives a solace element to the exploring offices that regardless of the possibility that the ITA part of the case is lost, the denounced can't escape from the IPC part.

V. CYBER CRIMES: EUROPEAN PERSPECTIVE

In 1997, the Council of Europe [5] (COE) shaped a Committee of Experts on Crime in Cyberspace and met in mystery for quite a long while drafting a worldwide arrangement entitled the "Tradition on Cybercrime," (the Convention) that was discharged in definite frame in June 2001. Albeit thirty-four nations taken an interest in the formal demonstration of marking the Convention in November 2001, just six have endorsed the Convention. No real European nation has consented to be bound by the Convention. The main nations which have approved it are Albania, Croatia, Estonia, Hungary, Lithuania, and Romania. On November 17, 2003, President Bush transmitted the Convention, alongside the State Department's cover the arrangement, to the US Senate with a view to getting its recommendation and agree to endorsement. To wind up plainly authoritative on the US, the arrangement requires an endorsement of 66% of the Senate. At the point when the Senate considers a settlement, it might endorse it as composed, support it with determined conditions, reservations, or understandings, reject and return it, or keep its entrance into compel by withholding endorsement. The Senate's thought of a settlement is typically facilitated and for the most part takes maybe a couple years. Presently, the

Senate Committee on Foreign Relations has booked a hearing on the Convention on Thursday, June 17. [5] The Convention is an aggregate reaction by individuals from the Council of Europe (46 States) and some non-part States to the test of digital crime. It is the aftereffect of 4 years of serious work by a specialist committee, which was depended by the Committee of Ministers to set up a legitimately restricting instrument considering past Council of Europe suggestions on PC crime and criminal system issues connected with data innovation.

VI. THE COUNCIL OF EUROPE'S CONVENTION ON CYBER-CRIME

The Convention's principle goals were to:[6] set down basic meanings of certain criminal offenses so enactment can be fit at national level; characterize basic tenets for investigative forces which are suited to the data innovation condition; decide both customary and new sorts of global participation with the goal that nations can co-work quickly in their examinations and arraignments, e.g. by utilizing a system of changeless contacts.

VII. CRIMINAL OFFENCE

The initial segment of the tradition concerns criminal offenses, which put forward regular definitions. It is normal that, if appropriately actualized by contracting States, these definitions would wipe out issues of double guiltiness. These 9 offenses, a large portion of which were at that point characterized in the 1989 proposal on PC related crime, fall into four classes: offenses against the classification, respectability and accessibility of information or PC frameworks; PC related offenses; content-related offenses; and offenses including the encroachment of licensed innovation and related rights.

A. The First Category

There are four offenses in the principal classification. They all worry offenses whose essential target is the PC framework or information; in this manner, their indefensible nature is firmly connected to the PC condition in which they occur. Albeit some of these offenses may have an equal in the normal world (for instance illicit get to or "hacking" can be contrasted with the infringement of the home), making them offenses depended on an unmistakable criminal arrangement thought to ensure PC systems and the information they contain. [7] The real or potential harm caused by such PC offenses ought not to be thought little of. Breaking into a PC framework and presenting an infection can undoubtedly prompt the pulverization of information or whole frameworks everywhere throughout the world because of the interconnection of networks. Be that as it may, keeping in mind the end goal to be viewed as an offense, the lead must be conferred purposefully and unlawfully, i.e. "without rights". Henceforth, there are acts which, if properly approved and executed by the state experts (law authorization, insight or legal) or acknowledged as legal business practices, won't be viewed as a criminal offense under the Convention. Offenses in the primary classification are alluded to as "**Offenses against the privacy,trustworthiness,and accessibility of information or data frameworks**". They incorporate illicit get to, or "hacking" (otherwise known as "splitting" or "PC trespass"), which the Convention considers a gauge offense as it might prompt different offenses, for example, unlawful access to private information (counting passwords, data about the focused-on framework), utilization of the framework without payment and different types of PC related misrepresentation or imitation. Numerous national enactments as of now contain arrangements on "hacking" offenses, however, their degree and constituent components fluctuate significantly. Certain nations apply a tight definition or require extra qualifying conditions. Under the Convention contracting

states should criminalize unimportant hacking or, on the other hand, can append any or the greater part of the qualifying components recorded: encroaching safety efforts, extraordinary plan to acquire PC information, other untrustworthy goal that legitimizes criminal culpability, or the necessity that the offense be carried out in connection to a PC framework that is associated remotely to another PC framework. The last choice enables contracting states to reject the circumstance where a man physically gets to a remain solitary PC with no utilization of another PC framework. They may confine the offense to unlawful access to arranged PC frameworks (counting open systems given by media transmission administrations and private systems, for example, Intranets or Extranets). Another offense in this classification is an unlawful capture attempt, which is demonstrated on the infringement of the protection, for example, **tapping and recording of oral phone discussions,** and applies this rule to all types of electronic information exchange, regardless of whether by phone, fax, email, or document exchange. The offense applies to 'non-open' transmissions of PC information. The term 'non-open' qualifies the way of the transmission (correspondence) handle and not the way of the information transmitted. The information imparted might be freely accessible data, yet what makes a difference is that the gatherings wish to convey secretly. Or, on the other hand, information might be kept the mystery for business purposes until the administration is paid, as in Pay-Tv. Subsequently, the term 'non-open' does not per prohibit interchanges by means of open systems. Be that as it may, in a few nations, block attempt might be firmly identified with the offense of unapproved access to a PC framework. Keeping in mind the end goal to guarantee consistency of the preclusion and utilization of the law, nations that require unscrupulous plan, or that the offense be perpetrated in connection to a PC framework that is associated with another PC framework as per the arrangement of illicit get to, may likewise require comparable qualifying components to join criminal risk in this offense.

The arrangement on information impedance tries to give PC information and PC programs with assurance like what is delighted in by mortal items against deliberate harm. Lead constituting the offense, for example, **harming, weakening or erasing PC information,** include a negative modification of the honesty or of data substance of information and projects. The contribution of information, for example, malignant codes, infections (e.g. Trojan stallions), is additionally secured, like the subsequent adjustment of the information. The arrangement on framework obstruction criminalizes demonstrations of PC damage. The offense comprises in the purposeful obstructing of the legitimate utilization of PC frameworks, including media communications offices, by utilizing or affecting PC information. The content is detailed impartially so that it can ensure a wide range of framework capacities. The expression "impeding" alludes to activities that meddle with the correct working of the PC framework. Such preventing must occur by contributing, transmitting, harming, erasing, adjusting, or smothering PC information. Rather than information impedance, the preventing of PC frameworks must be "not kidding" keeping in mind the end goal to be viewed as a criminal offense. Each contracting state should figure out what criteria must be satisfied all together for the obstructing to be viewed as "genuine." For instance, a state may require a base measure of harm to be caused all together for the frustrating to be viewed as genuine. The Council of Europe specialists considered as "genuine" the sending of information to a specific framework in such a shape, size or recurrence that it has a huge impending impact on the capacity of the proprietor or administrator to utilize the framework, or to speak with different frameworks (e.g., by methods for projects that create "foreswearing of administration" assaults, noxious codes, for example, infections that anticipate or significantly moderate the operation of the framework, or projects that send colossal amounts of

electronic mail to a beneficiary so as to square the correspondences elements of the system).This arrangement on the abuse of gadgets builds up as a different criminal offense some particular lead (generation, dissemination, deal, and so forth.) in regards to getting to gadgets which were fundamentally planned or adjusted for

abuse. Gadgets that are composed and utilized for lawful objects are not caught. (It was bantered finally whether the gadgets ought to be limited to those which are composed solely to commit offenses, along these lines barring double use gadgets, yet this was thought to be excessively tight. Such a definition could have prompted outlandish troubles of evidence in criminal procedures, rendering the arrangement for all intents and purposes inapplicable or just pertinent in uncommon occasions.) This offense, along these lines, requires a specific reason, i.e., carrying out any of alternate offenses against the privacy, the honesty, and accessibility of PC frameworks or information, as characterized in the Convention. As the commission of these offenses regularly requires the ownership of methods forget to ("programmer instruments") or different devices, there is a solid impetus to obtain them for criminal purposes, which may then prompt the making of a sort of underground market in their generation and dissemination. To avert more perilous results, the Council of Europe consented to forbid at the source direct identified with the creation, conveyance, deal, and so on of such gadgets, going before the commission of other PC crimes. Further, the unimportant ownership of such gadgets or get to codes is likewise criminalized.

B. Second Category

Offenses in the second class cover PC adaptations of two offenses (**extortion and fraud**), [8] which are typically executed in the customary way, in the physical world. By the by, misrepresentation or fabrication can likewise be executed on PC systems, which thus turn into the methods by which the offense is submitted, rather than being its objective. Both are essentially control based lead. It is important to make such direct separate criminal offenses as the meaning of customary structures – with respect to most national laws – infers that these can't be connected to acts executed through PC systems (for instance, because PC helped extortion, the component of misleading is missing and because PC supported imitation, the distinction between a unique and a duplicate at no time in the future exists). To be sure, with the entry of the mechanical unrest the open doors for perpetrating monetary violations, for example, misrepresentation, including Visa extortion, have duplicated. Resources spoke to or regulated in PC frameworks (electronic assets, store cash) have turned into the objective of controls like conventional types of property. These violations comprise for the most part of info controls, where off base information is sustained into the PC, or by program controls and different impedances with the course of information handling. The point of the arrangement on PC related misrepresentation is to criminalize any undue control (counting input, modification, cancellation, concealment of information and additionally obstruction with the working of a PC program or framework) over the span of information handling with the expectation of acquiring an unlawful exchange of property. The point of the arrangement on PC related phony is to make a parallel offense to the falsification of unmistakable records. It goes for filling holes in criminal law identified with customary imitation, which requires visual comprehensibility of articulations, or presentations encapsulated in an archive and which generally does not make a difference to electronically put away information. Controls of such information with evidentiary esteem may have an indistinguishable genuine outcome from customary demonstrations of imitation if an outsider is in this manner deceived. PC related

phony includes the unapproved creation or change of put away information with the goal that they obtain an alternate evidentiary esteem and the course of lawful exchanges, which depends on the genuineness of the data contained in the information, is liable to a double dealing.

C.Third Category

The third category of offenses identifies with **illicit substance and incorporates various acts** identified with youngster pornography. [9,10] When drafting the Convention, the Council of Europe has distinguished this classification of an unlawful substance as the most hazardous one with regards to PC systems, which required tending to by criminal law provisions. The tradition as needs is made different acts going from the deliberate ownership to the generation and dissemination of kid explicit entertainment criminal offenses, in this way covering every single conceivable connection in the chain. Regardless of exceptional endeavors, different sorts of illicit substance, specifically bigot publicity, were excluded among substance-related offenses in the tradition itself, yet had been included later in a supplementing protocol. The arrangement on kid smut tries to reinforce defensive measures for youngsters, including assurance against sexual abuse, by modernizing criminal law arrangements that outline the utilization of PC frameworks in the commission of sexual offenses against kids. Most States as of now criminalize the conventional creation and physical dispersion of tyke explicit entertainment, yet with the steadily expanding utilization of the Internet as the essential instrument for exchanging such material, it was felt that arrangements in a global lawful instrument were fundamental to battle this new type of sexual abuse and risk of kids. It is broadly trusted that such material and on-line rehearses assume a part in supporting, empowering or encouraging sexual offenses against youngsters.

D. Fourth Category

The fourth classification of offenses includes **encroachment of copyright and related rights** through PC systems. [6,11]. This class is additionally connected to content, however, content which is legitimate and ensured. Encroachments of licensed innovation rights, specifically of copyright, are among the most regularly dedicated offenses on the Internet, which may cause generous damage vow to copyright holders and the individuals who work professionally with PC systems. The generation and spread on the Internet of secured works, without the endorsement of the copyright holder, greatly visit. Such ensured works incorporate artistic, photographic, melodic, varying media and different works. The simplicity with which unapproved duplicates might be made because of advanced innovation and the size of multiplication and scattering with regards to electronic systems made it important to incorporate arrangements on criminal law endorses and upgrade worldwide collaboration in this field. The Convention gives that Parties need to criminalize wilful encroachments of copyright and related rights, at times alluded to as neighbouring rights, emerging from the assertions recorded in the article (e.g. TRIPS and WIPO Copyright Treaty) when such encroachments have been conferred by methods for a PC framework and on a business scale.

VIII. THESE OBSERVATIONS ARE MEANT TO ILLUSTRATE THE FOLLOWING

✓ International consensus on rules for cyberspace will still be difficult to achieve given strong and often diverging (national) interests.

✓ An all-inclusive international agreement encompassing cyber (or information) warfare, terrorism and crime as proposed by some states would hardly be feasible.

On cybercrime as a matter of criminal justice, not much progress has been achieved by the UN-GGE since 1990, while the Budapest Convention is in place and functioning.

IX. CONCLUSION AND DISCUSSION

Increment money related support to activities for enhanced preparing of law authorization and legal specialists versus the treatment of cybercrime cases and make a move to organize all multinational preparing endeavours in this field by the setting up of a preparation stage. Bolster explore useful to the battle against cybercrime. Proceed and create work, focused on zones, for example, in the Fraud Prevention Expert Group on the battle against misrepresentation with non- money methods for payment on the Internet. Proceed with arrangements and propose fundamental enactment against unlawful substance, particularly in regards to kid sexual mishandle material and prompting to psychological warfare, on the Internet.

- **Ambiguous Terms**

Vital terms in the law are not plainly characterized. This is perilous as it might have different degrees of translation.

- **Threatens Freedom of Speech**

The vagueness of the arrangements, especially the online defamation, can make individuals be careful about what they say on the web. The composition of reality might be viewed as slanderous, contingent upon the way it is dealt with. To put it plainly, individuals are intuitively being controlled by the law. Regardless of the possibility that the right to speak freely is not boundless, the law still hinders by one means or another, those people that need to stand up. There is a dread that any negative remark and feedback might be viewed as an "assault," and can be utilized against them.

- **Maintenance of the Law**

The usage and execution of the Cybercrime Law would alone cost of it. Also, the genuine arraignment of it. The Cybercrime law manages fragile topics and must be taken care of with adjust and objectivity to make it work.

REFERENCE

1. http://www.legalindia.com/cyber- crimes-and-the-law/
2. International Journal of Engineering Science and Computing, April 2016: CyberCrimes: An Indian perspective, Mayank R. kothawade[1], Prof. Dr. Preeti Agarwal[2].
3. India: An Overview Of Cyber Laws vs. Cyber Crimes: In Indian Perspective
4 International Journal of Advanced Research in Computer Science and Software Engineering, August 2013: Online Banking Security Flaws: A Study, Rajpreet Kaur Jassal, Assistant Professor., BBSBEC Fatehgarh Sahib, India. Ravinder Kumar Sehgal, Principal, JSSIET, Kauli, Patiala, India.
5. Marion, N. E. (1997). Symbolic Policies in Clinton's Crime Control Agenda. Buffalo Criminal Law
6. Council of Europe. 2001. 'Convention on Cybercrime (Budapest Convention).' As of 12 October 2015
7. Council of Europe. 2015a. 'Convention on Cybercrime: Status as of 24/8/2015.' As of 12 October 2015:
8. Council of Europe. 2015b. Assessment report: Implementation of the preservation provisions of the BudapestConvention on Cybercrime. Cyber Crime Convention Committee, June 21. As of 12 October 2015
9. Council of the European Union.n.d. 'Strategic guidelines for justice and home affairs.' As of 12 October

2015.

10. Council of the European Union.2014a. Outcome of Proceedings – EU Cyber Defence Policy Framework. As of 12 october2015 /sede160315eucyberdefencepolicy framework_en. Pdf
11. Council of the European Union. 2015d. 'CEPOL: Council and Parliament agree on updated rules.' Press Release 544/15, 30 June. As of 12 October 2015:
http://www.consilium.europa.eu/en
press/press-releases/2015/06/30- cepol-updatedrules/

About authors

Mohankumar.M is pursuing his Ph.D. at Karpagam University, Coimbatore. His area of research interest Software Engineering, Green Software Engineering, Cyber Security-His professional qualifications include MCA from Bharathidasan University. He has a working experience of 9 years in Karpagam University as Assistant professor. Organized workshops, FDP, guest lecturing he was interested.

Venkatesan.**S** received the B.Sc. degree in Computer Science from Karpagam University and pursuing and he is M.sc computer Science at Karpagam University, Coimbatore. His area of research was Cyber Security, Digital Image Processing, Software Engineering He has attended National Level Workshop, International Seminar, and International conferences.

Malarvzhi.V received the B.Sc. degree in Information Technology from Karpagam University and she is pursuing her M.sc computer Science at Karpagam University, Coimbatore. Her area of research was Cyber Security, Digital Image Processing, Software Engineering. She has attended National Level Workshop, International Seminar, and International conference