SUPREMO AMICUS

VOLUME 4 ISSN 2456-9704

CYBER SPACE THE DOUBLE-EDGED SWORD

By *Prachilekha Sahoo*
From *University Law College, Utkal University*

Introduction

Man is a social animal and it has a natural tendency to want to communicate and socialize. Once he realized the significance of using computer network to communicate, he began to demand access. Cyberspace is the biggest breakthrough mankind has ever seen and experienced in the field of science and technology. It is so vast and colossal that it becomes impossible to fathom it as an invention. From being unknown to absolutely ubiquitous, cyberspace has morphed from military communication to global phenomenon. It is a veritable outhouse on clicks from which one can transcend to some other place virtually. The paper takes a broader aim to know how the cyberspace has catered to thrive as a double-edged sword. It has shed light on the emergence of cyberspace and the history behind it, the advantages and the disadvantages has been drawn upon with some contemporary case studies. Following which how cybercrime has emanated and combated with the existing law.

Cyberspace and its history

Theword 'cyber' has its origin from the Greek verb "Kubernao",which means "to steer". William Gibson, a science fiction author first coined the term 'cyberspace', when he sought a name to describe his vision of a global computer network, linking people, sources, information and machines altogether, through which one can wander or navigate in a parallel universe. The Merriam Webster dictionary meaning of 'cyber' is 'relating to or involving computers or computer network'. Cyberspace means "The notional environment in which electronic communication occurs or virtual reality."[1] In simpler explanation it is a world comprising of optical fibers, digital signals, data, bytes and other such elements that maybe thought of, together, constitutes cyberspace/cyber world/internet.[1] It is a world within a world, inhabiting persons from every nation on earth with no defined geography and chorography, spreading across the globe and is of only four decades old. It has the population of 3.2 billion people or almost half of the world's population, surpassing any nation (China, India etc.). Although it feels like the internet has been around us since time immemorial but it has been only around us for over 40 years. It all began in the United States as a University experiment in military communications during the cold war. It was decided to link computers together in a network instead of perfectly aligned straight line. The Pentagon had this notion that if there is a nuclear strike on the USA, it was unlikely to damage the entire network and therefore there is still a chance that they would be able to send and receive intelligence.

At first, the computers were physically linked to each other but this method had its own limitations. This problem was solved by the development of usage and utilization of telephone network system. They deduced that, even if there is a nuclear strike or not, they can still talk to each other using this computer network. Gradually it was seen that some university student started using this network system to do their homework together. At first the users were primarily from the university and government sectors. Increasingly all sector of people became a daily part of it in one way or other. It was started to herald as the next big thing. More and more people could see the endless possibilities of computer networks in different dimensions and it started to grow rapidly. The internet has been renovated from an esoteric communication system for the military and scientific elite to a massively prevalent medium.

The launch of the Educational Research Network (ERNET) in 1986 established as the first step in the history of the internet in India. The network was strictly made available to educational and research communities. Two years later, in 1988, NICNet was established for communications between government institutions. The network was operated by the National Informatics Centre. On 14th August, 1995, the first publicly available internet service in India was launched by state-owned VSNL for commercial purposes.[1]

Advantages/ Case studies

The world of internet has no limiting scope and expands up until, till the mind can perceive. During the last four decades, this space has grown from one-dimensional approach to multi-dimensional approach. It has grown tremendously and matured into a popular medium, visited by millions of people stretching it each day to new vistas. It has enabled people to interact and communicate with each other, exchange data and information, share ideas, entertain, do trade and commerce, plan, confer and scheme things accordingly. The magnum opus of a digital transformation network and innovation, for its 'anytime, anywhere' services, internet gives instant access to an endless supply of knowledge and entertainment. Internet makes the world smaller and closer, keeping people within each others reach.

In the Mahabharata era, Guru Dhronacharya, the revered teacher refused to take tribal prince Eklavya under his tutelage because he was not a high born from the lineage of royal family. To seek inspiration Eklavya made and instituted a statue of Guru Dhronacharya and practiced archery day and night. Now a student as dedicated and passionate as Eklavya could easily have found himself a virtual guru in this 21st century without having being worried about his lineage, caste and all other things. He simply would have excelled and would have saved himself from the embarrassment of playing favorites and biases.

In the age of cyberspace, education is easily availed through online platforms to enrich the minds of the students. They do not need to travel long distance or reside in faraway places for the search of quality education or coaching tutors. Everything is readily available in the internet and is just a few clicks away. Online education has grown so much at such fast pace as internet allows innovative tools for imparting education. Universities are offering distance courses to make studies more efficient and convenient.

Internet has become a favorite gateway for those who seek to learn but can't afford the price of living in distant foreign lands. Secondly, data and information are the biggest advantage that an internet offers. It is a virtual gem trove of information. On any topic, any kind of information is available and gets picked up under the sun on the internet. Using search engines, websites dedicated to any matter and bulky number of articles, paper services is available instantly on tap for perusal in a quick matter of few seconds. Students are able to finance their own education by working part time in online jobs such as data entry, creative writing, blogging etc. This not only helps them earn few bucks but also hones their skills. In fact, internet has acquired the sources to locate job opportunities and finding right talented individuals for any advertised organization.

Internet lets people to communicate with each other virtually in any part of the world, staying within a four walled room. The further addition of chat rooms and video-conferencing has made it more feasible and available. Different forums plenteously exist where people can voice their opinion, discuss, debate and can comment over any topic. Social Medias like Facebook, twitter, instagram etc. allows people to share their photographs or memories and cherish them together with their friends and relatives alike. With the establishment of these services mankind has forged a new global friendship sharing his thoughts, participating and exploring other worldly events and cultures.

Entertainment is another most popular aspect for people surfing the internet to kill their boredom. Playing online games, listening to songs or downloading the latest movies and watching them are some of the ways to pass time. Due to ingrown demand in the online gaming, enthusiastic gamers competing against each other from various parts of the world, the gaming industry has revolutionized to cater the needs of their consumers. Similarly, lining up in a queue for a latest music album is a thing of the past as they are live streamed over the internet, thus saving the time and effort.

E-commerce sector has boomed due to paradigm shift from traditional method of shopping to virtual medium. They have proliferated their bases in the countries and have gotten a complete makeover to attract and captivate their targeted set of consumers. With numerous options flooding over our computer screen, we have a world full of choices. From medicines to clothes, home furnishing equipment to automobiles, we have a plethora of options lurking around. One can select the desired product and the entire financial transaction is carried out and conducted through the internet. The majority of companies are therefore doing the right thing in defining their own role in this new virtual universe.[1]

Furthermore, transferring money is not a tedious, heckling job anymore. Banks have come up with online transaction services which have made our life expedient. Numerous online services now can perform all the transactions online. One can book tickets for movies, reserve a hotel, pay utility bills, taxes and transfer funds through the internet. Internet has transfigured our world with easier options.

Our increasing reliance on cyberspace and the internet is evident. We had over 100 million internet users in India over two years ago. Adding to this number, there are 381 million mobile phone subscriptions with internet connectivity and the increasing seamlessness with which all sorts of devices are connected to the internet. There are over 2 billion internet users in the world- a number that doubled in the five years between 2005 and 2010.The figures are growing exponentially every year.[1]

"If you want a free society, just give them internet access." These were the words of 30-year old Egyptian activist Wael Ghonim in a CNN interview on February 9, 2011, just two days before long-time dictator Hosni Mubarak was forced to step down under pressure from a popular, youthful and peaceful revolution.[1] The netizens of Egypt were successful in mobilizing the people through the 'Revolution of 25 January' , a virtual event on the social networking site: Facebook. It took the world by storm when the news hit the world about how the Egyptians were successful to overthrow the dictatorship government who ruled the country ruthlessly for close to three decades. Internet became a powerful tool for the citizens to unearth corruption, mobilize mass for protests and demonstrations and act as a real watchdog over the government. Internet helped to turn individualized, localized and community-specific dissent into structured movements with a collective consciousness about both shared grievances and opportunities for action.[1]

The role of internet in the creation of awareness is immense. It opened up possibilities for journalists, activists and bloggers alike to get involved in the creation of awareness among the public mass. It helped fostering a creation of a shared identity among larger group of women who were nonetheless concerned but never really channeled it into action. Another such example is "One Million Signature" campaign in Iran. The campaign aimed to collect one million signatures among men and women to support the change of discriminatory laws and to raise consciousness and awareness regarding the unjust nature of Iranian laws concerning to women. The Government increased its attacks on the women's movement as it garnered success in this initiative, both domestically and globally. Later on, the Iranian Government caved to their demands. Similarly in India, Anna Hazare effectively used internet and social media to mobilize the youth and middle classes in his agitation over the issue of Jan Lokpal Bill. The issue not only amassed a lot of attention in the cyberspace world but also got huge support from the anti-corruption campaigns worldwide.

The power and potential of cyberspace/internet is now widely recognized by the governments across the world. Internet provides social media as a platform to engage people and the government, cohesively together by seeking feedback, checking corruption and empowering people. The ruling government is changing the dimension of governance with the usage of internet. Political activism has paved a way for social activism.

Disadvantages and case studies

The mythical Roman God Janus has two contrast characteristics aspect to it. He is known as the God of beginning as well as the God of ending, often depicted with two faces. Therefore the Roman God Janus would be an apt metaphor to describe cyberspace. Cyberspace is a double-edged sword that we tread upon every day. Like every coin has two sides, similarly even the exponentially growing phenomenon has its own distinct downside.

Cyberspace the new frontier, is the common heritage of mankind but unfortunately some people misuse the common heritage and therefore, cyberspace is also a new frontier of different types of crime which is labeled as cybercrime.[1]

With the development of internet, and its related assistance also developed the cyber-crime. Cybercrimes are the new emerging species of crime. It has not been defined in any Act or statute passed by the Indian parliament. In general term cyber-crimes are crimes which are perpetuated against people where cyber space serves as the medium. The computer can be used as a tool or a target or both. Cyber-crimes are different than the conventional crimes, sometimes fathomless and as heinous as it could be. It promotes anonymity, albeit unintentionally. There is nothing similar between a conventional crime and a cybercrime. Cybercrimes often go unnoticed, undetected and unreported due to its anonymity feature. Cyberspace facilitates anonymity encryption which again in most of the cases is devastating to criminal investigations. Within a split second cybercrime can be committed in any part of the world. Cybercrimes are scene less, deducing evidence needs exquisite skills which need specially trained hands to detect, recover, conclude and analyze the digital evidence. Cybercrimes are borderless. It can transcend state and national boundaries, in no time.[1] The concept of jurisdiction becomes irrelevant here as the whole world is a crime field. There are no eyewitnesses, no physical violence as there is no crime scene. Most of the time realization hasn't dawned upon the victim that he was hit with blows swift, silent and with a killer punch.

Also hiding behind a fake name or remaining anonymous gives people a bolder persona that they couldn't have achieved had been they face to face or in reality. There is always a lookout for gullible and unwary people browsing online so that they can be lured and tangled in a web of deceit. Personal photos and data/ information can be used against those persons for dubious purposes, making them emotionally wrecked and helpless. Also pedophiles lurk around with fake identities befriending with the innocent children and later kidnapping them to satisfy their perverse minds. Often such cases go unreported due to the stigmatized fear.

A few years back, there was lack of awareness about the cyber-crimes and its reach. India is not far too behind to catch up with it. As per the reports of National Crime Records Bureau (NCRB), 11,592 cases of cybercrime were registered in India leading to 8,121 arrests. Among the states Uttar Pradesh is in the lead with highest number of cyber-crimes at 2,208 while Maharashtra is placed second closely with 2,195.Every ten minutes in India at least one cybercrime is reported in the first six months of 2017 compared to twelve minutes in 2016.

The recent rumors that mongered about communal violence between Hindu and Muslim in Kolkata which created a massive furor, sets an example on how this tool, with its unrivaled reputation as an information assassination can suffer if internet facilities are abused, especially by those who have an axe to grind.

Recently the world was caught up in a whirlwind with the ransomware virus. Global Ransomware attack affected organizations around the world including Britain's National Health Services. The criminal hackers found a loophole in 'retired' Microsoft software which was not routinely scrutinized for update and patched for security, thus infecting computers with the Wannacry Ransomware virus. Ransomware is a type of malicious software designed with the intent to block the access to any computer system, until the ransom money is paid by the owner as demanded in online crypto currency bit coins. The software attack took a toll on the entire world affecting biggest of nations and organizations posing a major threat to them.

Another game that consumed the world into horrors of cybercrime happens to be the blue whale game. The Blue Whale Challenge is a morbid social media game targeting vulnerable youngsters and pushing them to inflict self-harm and ultimately suicide. The challenge involves 50 tasks given by the administrator and has to be completed one by one. The game usually preys on teenagers and young adults, people who are susceptible to influences and attempts to create a thin air of unworthiness and ineptness around them. The game requires players to submit sensitive data before playing the game, which the administrators use it against them to blackmail if else the players try to back out. The game was launched in Russia in 2013 and its inventor is currently behind the bars. Yet the authorities are unable to control its spread.

Nigerian Advance Fee Fraud or Advance-fee fraud schemes are a very common online cybercrime fraud which is committed by spam-bots. Spam bots, as the name suggests, are artificial intelligence bots that have been programmed to "spam" or send multiple emails to those users who have lower email security measures and are susceptible to online attacks. Although such scams originate from the world over, it came to prominence while being associated with a sender claiming to be a powerful Nigerian political figure requesting cash is wired to him to help him out of a problematic situation. The spam-bot creates vividly detailed and human-like emails soliciting potential victims to wire in a certain amount of cash which would then allow the sender to reimburse any person who helps him by a deposit of money much larger than the amount originally borrowed. By doing so the perpetrator gains access to multiple points of personal detail of the victim and uses this information to further drain money, utilize benefits requiring the victim's online signature and so on. These perpetrators then gain access to a wide range of personal information and threaten to misuse or physically harm the victims should they try and retaliate or complain to law enforcement officials. Some victims have even been lured into the country of Nigeria where they were imprisoned, kidnapped or worse. While very easily recognizable in the modern day by most people as a hoax, at the time of its initial launch into the World Wide Web, it was a cybercrime of epidemic proportions that lead to millions of dollars’ worth of loss for countless victims worldwide. The Nigerian government however is unsympathetic towards the victims as the victims themselves, by following instructions, are punishable by law for conspiring to remove funds from Nigeria in an illegal manner. Victims who are somehow able to escape dire consequences suffer debt, damage to credit rating, identity theft or face legal action on an international level. This fraud is a perfect example of a combination of advance fee fraud and identity theft. To avoid advance fee fraud individuals and organizations need to be vigilant and follow some basic steps in verifying emails which include any form of solicitation involving funds. One must never reply to a mail from a third party who is not involved with a person you know personally or a client you are dealing with. Push the perpetrators for information which in turn with makes them give you more info to file a suit against them later on. And under no circumstances should any amount of form of money is to be sent across to anyone until such perpetrators have been completely shielded off from your online presence. Recently the rise of artificial intelligence security systems that automatically sense and adapt to incoming threats have reduced such fraud to a great extent. But as can be seen from latest organization wide surveys, human errors still account for a majority of such cybercrimes. So the only fool-proof way to protect individuals and organizations from such fraud is in-depth training and awareness.

Internet has kept the tarred reputations of public figures, infringed laws of privacy, copyright and other human rights through user-generated content. Yet in no way it has deterred the growth of the phenomenon which has threatened to replace traditional method whether in India or any country in the world. Despite facing criticism that internet has adversely affected personal communication whereby people no longer seem to find the time to talk to each other in face to face, old-fashioned way, the virtual space keeps throwing up newer and more engaging means of networking.

Analysis of Indian Cyber Law

Cyber-crime is pernicious in nature and has taken the world under its grip. It is confronting our planet with questions which no nation can seem to answer. A cyber-criminal can easily hack the websites and portals, plant viruses and carry out cyber frauds. He/ She can penetrate into highly classified and confidential files; bring out sensitive matters which can endanger a nation’s security. Cybercrimes are exponentially growing by each day, throwing up new challenges for the law and order machinery. It causes economic loss and risks to countries, undermines development opportunities and threatens international peace and stability.

Cyber-crime includes phishing, bank robbery, child pornography, cyber terrorism, credit card frauds, cyber stalking, industrial espionage, scams, hacking, kidnapping children via chat rooms, creation and /or distribution of viruses, spam and so on. Cyber-crimes have been divided into two categories:-

i) The crimes in which computer is the target. Examples- hacking, virus attacks etc.

ii) The crimes in which computer is used as a weapon. Examples – cyber terrorism, pornography etc.

The Convention on Cyber-crime or Budapest Convention is the first and only binding multilateral treaty which is based on combating cybercrime. The Council of Europe drafted it with active participation from the observer states in 2001 providing a framework for international cooperation between the state members of the treaty. The object of this substantive multilateral treaty is to address cybercrime with convergent, harmonized legislation, capacity building and cooperation, enjoying compliances even from the non-signatory states. India has taken a cue from the developed countries and is one of the few countries to take steps to counterattack cybercrimes.[1]

Heading in this sphere, India has taken a roadmap to full-fledged legal system to ensure that the administration of human conduct is regulated in cyberspace and proper policies are formulated.

In 1996, the UNCITRAL, i.e. the United Nations Commission on International Trade Law adopted the Model Law of electronic commerce followed by the United Nations' General Assembly recommending all the states to give favorable considerations to the State Model Law when they enact or revise their laws by its resolutions bearing NO. 51/162. [1] The Indian government also realized the need for legislation and came out with Information Technology Act, 2000. It was the first Act to define cybercrime and provide for penalties, punishment and compensation in the listed crimes in the Act itself.

• The objective of this Act was to accord a legal sanctity to all the electronic records and activities carried out by electronic means or better commonly known as e-commerce. It facilitated electronic filing of the documents with the government agencies.

• The above implications of the provisions will enable the e-mail to exist as a valid and legal form of communication, which can be duly produced and proved in a court of law.

• Under IT Act, 2000, extra company notes and memos which was used for official purposes, shall also come under it.

• The Corporate sector thrives on e-mails and digital signatures on a regular basis to carry out their tasks online. Under the ambit of IT Act, 2000 secure digital signatures have got legal validity. When in dispute over the digital signatures, such signatures are to be authenticated by the Certifying Authority which is further overseen by a Controller of Certifying Authorities.

• The Corporate sector before the advent of IT Act had no legal redressal for issues concerning cybercrimes such as hacking, damaging the computer core etc. Now, the Act has provided remedy in form of monetary compensation amount not exceeding up to Rs 1,00,00,000.

• Many cybercrimes has been defined and has been declared penal offences punishable with imprisonment as well as fine.

• Further the amendment of Indian Penal Code (1860), Indian Evidence Act (1872), Banker's Book Evidence Act (1891) and the Reserve Bank of India Act (1934) to be done so as to bring them in consonance with the information technology regime.

• This Act also provided for the Cyber Appellate Tribunal to be set up to hear appeals against adjudicating authorities.

Although the IT Act, 2000 has proven to be a success but it also has its fair share of criticism. The negative aspects are as follows:-

• Exclusion of negotiable instruments from the applicability of IT Act, 2000. The Act promotes electronic commerce whereas a payment received by means of negotiable instrument for an e-commerce transaction doesn't get included in the ambit of Act.

• The IT Act, 2000 doesn't deal with the protection of Intellectual Property Rights in the cyberspace which is one of the biggest blunders.

• There is no uniformity/ balanced approach regarding the degree of the crime to that of the punishment which makes it appear out of sync with other principles of criminal law.

• Under the IT Act, 2000 no difference has been made between ethical and unethical hacking, and has mandated it as punishable offence. RBI in its guidelines, dated June 14, 2001 had encouraged all the banks to utilize the services of 'ethical hackers' for accessing the shortcomings in the security system. This shows the irony of the law.

• Many other forms of cybercrimes have been left out or had no mention in the Act at all such as cyber stalking, cyber forgery, spamming etc.

• The IT Act doesn't define the offences if they are bailable or non-bailable in nature, compoundable or non-compoundable.

• It hasn't laid down parameters for its implementation.

The IT Act, 2000 was amended in 2008, which introduced remarkable provisions and amendments facilitating the effective enforcement and growth of cyber law in India. Data protection is of utmost importance and finds it rightful place in S-43, 43A, 66, 72 of the Act. Plethora of cybercrimes have been incorporated under Chapter IX as offences under the Amended Act such as cyber terrorism, child pornography etc. The offences have been defined if they are bailable or non-bailable, cognizable or non-cognizable.

Even though some of the pressing matters have been addressed, there is still a long way to cover all the lacunas. With the crime infiltration growing rapidly we need to march fast and ahead so as to control its menaces. After discussing the challenges before Indian cyber law regime, some strategies needs to be employed.

• To educate the netizens and common man about their rights and obligations in the cyberspace. The concerning fact is that most people are oblivious of the laws of the cyberspace, the crimes that lurks around and the forums for redressal of their grievances.

• It should be obligatory to impart the basic legal and technical training to law enforcement officials.

- There must be a cybercrime cell in vicinity of every local police station as it is often said accessibility is the greatest impediment in delivery of expeditious justice.

- There is only one government recognized forensic laboratory in India at Hyderabad which prepares forensic reports in cybercrime cases. We need more such labs to efficiently handle the increasing volume of cybercrime investigation cases.[1]()

- Adoption of foolproof security procedures of computer in organizations.

- International interaction and information exchange between countries to provide, practical, effective and comprehensive solutions.

Conclusion

Cyberspace has always been a double-edged sword. It has enabled exponential growth and unparalleled advancements in various sectors, at the same time it has led to overload of data and risking personal security. Our every move is tracked, for better or for worse. Sometimes they help us enhance our experiences and make the best of what we have but sometimes, with a hint of human malice, the same technology can put us into grave trouble. Take for instance the prevalence of frauds, phishing and identity theft in cyberspace. At the click of a few buttons and a momentary lapse of attention, our entire identity and all associated entities related to it are snuffed out and exploited. With cyberspace came the prevalence of cloud computing and with cloud computing came the problem of transparency. Various entities can poke and prod through our cyberspace history and data and may decide to use it against us. With e-commerce came the era of customer driven, easy to order business but with it also came frauds and cases of theft. In a world where data is free flowing in every form through every space, in an era where the Internet of Things and automation are the go to technologies, security and security enforced with lawful intervention is of paramount importance. With laws at nascent stage prevalent in our judicial system we cannot possibly fathom facing global cyber space threats like electronic warfare, large scale hacking and other such activities because not only is the jargon and vocabulary required to handle these situation not present, but getting such legislations and amendments through quickly enough to react to rising global threats is going to be a herculean task. Both in terms of the administration and the populace. The administration needs to understand and fast track the proceedings dealing with such cyberspace crimes and the populace needs to be made aware of all the benefits and protections they have in place to deal with in case things get out of hand. Lastly, we need to ask ourselves the ever-pertinent question, is the cyberspace inherently malicious? The same dark web that enables our militaries to be technologically operational under the enemy radar is also the dark web that is used to distribute child pornography. The same crypto currency that is being adopted worldwide can also turn out to be yet another money-making hoax. The fact of the matter is that the cyberspace only turns hostile if the people in charge of it are hostile. Like every invention cyberspace is the manifestation of human ideas and action put together for the benefit of human society. Likewise, human beings are the only ones who have been bestowed upon with the ability to think, to work and to bring changes so the world is benefitted out of it. If the same minds can find a way to hack into top secret government databases, so can they provide countermeasures to not only combat such breaches but also back them up with legal enforcement so those who misuse such technology face the consequences of their wrongful actions.

Reference :

1. An Introduction To Cyber Law book *by Dr. J. P. Mishra*
2. Cyber And Criminal Law *byDr. Amita Verma*
3. Yojana Magazine *may 2013 edition*
4. Yojana Magazine *February 2017 edition*

*****