Scholarly Research Journal for Interdisciplinary Studies,
Online ISSN 2278-8808, SJIF 2016 = 6.17, www.srjis.com
UGC Approved Sr. No.45269, SEPT-OCT 2017, VOL- 4/36
10.21922/srjis.v4i36.10013

CYBERCRIME: BIGGEST THREAT TO NATIONAL ECONOMY AND SECURITY

Arun Verma

Research Scholar (Ph.D.), Assistant Professor of law, Invertis University, Bareilly

Email: verma.arun09@gmail.com

"Cybercrime" also consist of engaging in conduct that is outlawed because it threatens order, cyberspace differs from crime primarily in the way it threatens order. Cybercrime differs from crime primarily in the way it is committed: Criminals use guns, whereas cybercriminals use computer technology. Most of the cybercrime we see today simply represents the migration of real world crime into cyberspace. Cyberspace becomes the tool, criminals use to commit old crimes in new way[1]*....* ***Susan W. Brenner***

"**Cyber**" is a prefix used to describe a person, thing, or idea as part of the computer and information age, taken from ***kybernetes***, theGreek word for "**steersman**" or "**governor**," it was first used in **cybernetics**[2], a word coined by **Norbert Wiener**[3]and his colleagues. The virtual world of internet is known as cyberspace and the laws governing this area are known as Cyber laws and all the netizens[4,5] of this space come under the ambit of these laws as it carries a kind of universal jurisdiction. The cyber law can also be described as that branch of law that deals with legal issues related to using of inter-networked information technology. In short, cyber law is the law governing computers and the internet.

[1]Susan W. Brenner (2010) "Cybercrime: Criminal Threats from Cyberspace" Greenwood Publishing Group, Praeger P. 10. ISBN 978-0-313-36546-1

[2]Cybernetics is a transdisciplinary approach for exploring regulatory systems—their structures, constraints, and possibilities. Norbert Wiener defined cybernetics in 1948 as "the scientific study of control and communication in the animal and the machine." In the 21st century, the term is often used in a rather loose way to imply "control of any system using technology." In other words, it is the scientific study of how humans, animals and machines control and communicate with each other.

[3] An American mathematician and philosopher. He was a professor of mathematics at MIT.

[4]The term netizen is a portmanteau of the words Internet and citizen as in "citizen of the net".

[5]Seese, Michael. Scrappy Information Security. p. 130. ISBN 978-1600051326. Retrieved 5 June 2015.

Computer crime, or Cybercrime, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target[6]. Net crime is criminal exploitation of the Internet.[7]

The first recorded cybercrime took place in the year 1820. That is not surprising considering, the fact that the abacus which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan, and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.Today computers have come a long way, with neural networks and nanocomputing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second.

The Internet is a global system of interconnected computer networks that use the standardized Internet Protocol Suite (TCP/IP)[8]. It is a network of networks that consists of millions of private and public, academic, business, and government networks of local to global scope that islinked by copper wires, fiber-optic cables, wireless connections, and other technologies. The Internet carries a vast array of information resources and services, most notably the inter-linked hypertext documents of the World Wide Web (www) and the infrastructure to support electronic mail, in addition to popular services such as online chat, file transfer and file sharing, online gaming, and Voice over Internet Protocol (VoIP)[9] person-to-person communication via voice and video. The origins of the Internet dates back, to the 1960s when the United States funded research projects of its military agencies to build robust, fault-tolerant and distributed computer networks. This research and a period of civilian funding of a new U.S. backbone by the National Science Foundation spawned worldwide participation in the development of new networking technologies and led to the commercialization of an international network in the mid-1990s, and resulted in the following popularization of countless applications in virtually every aspect of modern human life.

---

[6]Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[7]Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.

[8]The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating by an IP network.

[9]Voice over Internet Protocol (also voice over IP, VoIP or IP telephony) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN).

Cybercrime is growing with our dependency on technology; today we can see technology everywhere whether in our kitchen room or office, or playground or in agriculture without software and hardware life seems impossible for us. We are so much dependent on technology that is why cybercriminals are causing lethal damages to our economy and security. This problem is much bigger than estimated; it can collapse theentire economy of any nation and can start a civil or world war. Cybercrime is a threat to so many things whether theeconomy, national security, privacy, intellectual property rights, and so many other things. Cybercrime is those crimes which are punishable under Information Technology Act, 2000. In another world,cybercrimeis those crimes wherein computer is either a tool or a target both.

IT revolution increased phonemically no of cyberspace users all over the world now India is on no 3 to use cyberspace. Internet Introduced in India starting with LaxmiNagarDelhi on 15 August 1995. Indian telecom industry underwent a high pace of market liberalization and growth since the 1990s and now has become the world's most competitive and one of the fastest growing telecom markets. The Industry has grown over twenty times in just ten years, from under 37 million subscribers in the year 2001 to over 846 million subscribers in the year 2011. According to Telecom Regulatory Authority of India (Trai) India's telecom subscriber base, mobile and landline combined touched the 1.18-billion mark at the end of February 2017). The number of Internet users in India is expected to reach 450-465 million by June, up 4-8% from 432 million in December 2016, a report from the Internet and Mobile Association of India and market research firm IMRB International said and in 2016-17, the government had estimated revenue of Rs98,994.93 crore from telecom sector, which included about Rs64,000 crore from spectrum auction and the rest from licence fees and other charges. From 2013 to 2015 the cybercrime costs quadrupled, and it looks like there will be another quadrupling from 2015 to 2019. Juniper Research[10] recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by2019, increasing to almost four times the estimated cost of breaches in 2015[11].

[10]https://www.juniperresearch.com/about-us
[11]https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#169d03313a91

There is anurgent need to study thebad impact of IT revolution on our society and economy and security of our nation, there is some personal and some pecuniary loss; both ultimately become thereason of human sorrow. To solve theproblem of cybercrime wemustfind out hacks and technologies of cybercriminal so that we can develop a strategy to stop cyber-attacks.

The demand of welfare state is not new to human civilization; it has been developed with the development of human civilization. Strong states are in aposition to make better welfare schemes and enforce them effectively. ***"Now power does not mean to have abig army, air force, Navel force or having abig nuclear arsenal but to have control over silicon chips, computer hardware/software and on cyberspace".***The service sector is booming by leaps and bound, it has abig share in countries GDP and revenue. There are some countries, their economy is solely based on service sector i.e. Switzerland. Imagine if any hacker hacks entire service sector of such country and make it impossible to work online. It will surely cause big harm to countries economy and ultimately that country will suffer financial emergency.

The same problem is with countries national security as we know defense services very much depend on technology thus there are great chances to hack defense and important government websites, which are crucial for national security by anenemy state. China government has acyber army to stop thecyberattack on their country and to hack important websites like adefenseof foreign countries especially India, USA, and Russia. ***Cyber warfare refers to politically motivated hacking to conduct sabotage and espionage.*** It is a form of information warfare sometimes seen as analogous to conventional warfare. Modern war is not awar of arms but its war of information and whoever has control over information will rule in themodern world. According to a top-secret survey report commissioned by the Indian government, nation's deepest military secrets are vulnerable to cyberattack, with 3,000 Internet connections of the Defense Ministry and the Air Force Communication Center at Vayu Bhawan having been compromised. Anonymous cyber hackers tried to hack India's defense deal with Russia in March 2014. There is ample evidence that shows that our defense deals are under cyber surveillance, therefore, we need to take all the necessary measures to curb these cyberattacks to protect our national security and defend our economic interests.

The threat of terrorism has posed an immense challenge in the post-Cold War period. Terror attacks in major cities, towns and tourist resorts across the globe have demonstrated the inadequacy of the State mechanisms to address this challenge. Serious attempts have been

made by Nations to address this challenge by designing counter terrorism strategies and anti-terror mechanisms. However, most of these are designed in a conventional paradigm, which might be effective in a conventional terror attack. However, there are limitations when it comes to a terror attack of an unconventional nature. The latest example of Assam and Muzzafarnagar riots are anexample of acyberattack in India.

Information technology (IT) has exposed the user to a huge data bank of information regarding everything and anything. However, it has also added a new dimension to terrorism. Recent reports suggest that the terrorist is also getting equipped to utilize cyber space to carryout terrorist attacks and recruitment. ISIS[12] has its separate cell to online recruit terrorist across the globe.The possibility of such attacks in future cannot be denied. Terrorism related to cyber is popularly known as 'cyber terrorism'.

In the last couple of decades, India has carved a niche for itself in IT. Most of the Indian banking industry and financial institutions have embraced IT to its full optimization. Reports suggest that cyberattacks are understandably directed toward economic and financial institutions. Given the increasing dependency of the Indian economic and financial institutions on IT, a cyberattack against them might lead to an irreparable collapse of our economic structures. And the most frightening thought is the ineffectiveness of reciprocal arrangements or the absence of alternatives. Cyber law is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace have some legal and cyber legal perspectives.

Cyber law encompasses laws relating to –

1. Cyber crimes
2. Electronic and digital signatures
3. Intellectual property
4. Data protection and privacy

As the Nation became successful in unearthing terrorist networks involved in the recently carried out terror attacks, the most outstanding feature was the use of the tools of the information age like emails, cell phones, satellite phones etc. to stay connected. The worrying aspect was the use of modern gadgets bringing out that the terrorist is not only obsessed with IEDs and AK-47, 57 but has also mastered the use of laptops and tablet PCs to give finesse to

[12]The Islamic State of Iraq and the Levant (ISIL), also known as the Islamic State of Iraq and Syria (ISIS).

his nefarious designs. As terrorist organizations realize its capability and potential for disruptive efforts at lower costs they will become more and more technology savvy and their strategies and tactics will have a technological orientation.

The wide range of existing estimates of the annual loss—from a few billion dollars to hundreds of billions—reflects several difficulties. Companies conceal their losses and some are not aware of what has been taken. Intellectual property is hard to value.

There are several components of malicious cyber activities which cause loss to national economy and security. I have divided these malicious activities into following parts:

1. The loss of intellectual property and business confidential information.
2. Cybercrime, which costs the world hundreds of millions of dollars every year.
3. The loss of sensitive business information, including possible stock market manipulation.
4. Opportunity costs, including service and employment disruptions, and reduced trust for online activities.
5. The additional cost of securing networks, insurance, and recovery from cyberattacks.
6. Reputational damage to the hacked company.
7. The loss of personal information that can cause pecuniary damages.

Put these together and the cost of cybercrime and cyber espionage to the global economy is probably measured in the hundreds of billions of dollars. To put this in perspective, the World Bank says that global GDP was about $4,41,64,405/- in 2017[13]. A $450 billion loss[14]—the high end of the range of probable costs—would be a fraction of a percent of global income. But this begs several important questions about the full benefit to the acquirers and the damage to the victims from the cumulative effect of cybercrime and cyber espionage.

As brought out earlier India has carried a niche for itself in the IT Sector. India's reliance on technology also reflects the fact that India is shifting gears by entering facets of e-governance. India has already brought sectors like income tax, passports visa, central government and state government's department and ministriesare under the realm of e - governance. Sectors like police and judiciary are yet not fully online. The travel sector is also heavily reliant on this. Most of the Indian banks have gone on full-scale computerization. This has also brought in concepts of e-commerce and e-banking. The stock markets have also not remained immune. To create havoc in the country these are lucrative targets to paralyze

[13]https://data.oecd.org/gdp/gdp-long-term-forecast.htm#indicator-chart
[14]https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html

the economic and financial institutions. The damage done can be catastrophic and irreversible.

Transnational Organized Crime (TOC) poses significant and growing threat to National and International security where dire implications of public safety, Public health, democratic institutions and economic stability across the globe. The cybercriminalhas extended their activities on the internet to de-stable government system and security.

According to a newly-released report sponsored by McAfee, global cyber activity is costing up to $500 billion each year[15], which is almost as much as the estimated cost of drug trafficking. In the U.S. alone, the report estimates that cybercrime is the catalyst behind the loss of as many as 500,000 jobs as companies grapple with the loss of coveted intellectual property, confidential strategies that are snooped on, and suffer reputational harm. This problem horrible in acountry like India where there is abig problem of unemployment and companies are struggling to survive in cut throat competition. Ultimately companies have other option to lay off or retrenchment to get rid of heavy losses of the company. "If workers displaced by cyber espionage do not find jobs that pay as well or better, the victim country would be worse off," the report said. "The effect of cyber espionage may be to move workers from high paying blue-collar jobs into lower paying work or unemployment."

If people have no job, then they can be indulged in sabotage and sedition activities which are harmful for any nation especially in acyber age where people can easily send confidential information over the internet to anyone either to aterrorist group or enemy country.

India is awitness of acyberattack on national security i.e. riots in Assam and Muzaffarnagar in U.P. and website of Army, Navy, Air force; Supreme Court of India and more than 30 important government website security, has been compromised by thecyberattack.

Cyber army of China and hackers (officially/unofficially appointed by theenemy state to hack those websites which are strategically important to get access to secret government files and projects) are causing damage to our economy and security. It is thebiggest challenge to our national security, economy and foreign relations, therefore, we need to take immediate precaution to protect our security and economic interest. There is adeep nexus between revenue and national security, without revenue government cannot spend ample money on defense and without good revenue, thegovernment cannot develop basic infrastructure and welfare schemes for citizens.

[15]http://www.business-standard.com/article/international/cyber-crime-costs-up-to-500-billion-to-world-economy-113072300596_1.html

Total loss caused by the cyberattack is much greater than our imagination that is why there is anurgent need to study real impact of thecyberattack on any nation. As we know that estimated yearly loss is about $ 500 Billion and this amount is big enough, total revenue of third world countries is less than this figure.

1. Cybercrime is an economic issue and is growing because of perverse economic incentives created by IT market, global economic trends, and the impact of laws.
2. A fundamental shift in security industry – economics is shaping security more than it ever has thus aloss in theeconomymeans cut in defense budget resulting in abigger threat to national security.
3. Cybercrime is biggest threat to privacy and security to government and private organizations, market, thestock market, individual and to thewhole society. Everyone bears consequences of cybercrime either directly or indirectly depending upon awareness of the people.
4. It is vital for our economic and national security to find out thereal figure of damage caused by cybercrime. It helps us to know theseverity of cybercrime and will help us to make more strengthen measures to curb cybercrime.
5. More research is necessary, good data would be a great start.
6. Outsourcing is totally depending upon cyber security and our economy is very much depending upon it, if Indian IT companies fail to provide quality service to our foreign clients then they will not invest in India and ultimately Indian government will suffer a huge revenue loss.
7. India and many other countries (especially third world countries) have invested millions of dollars to develop internet infrastructure and if there is no privacy and security over theinternet; no foreign investment will take place and finally government will bear that loss.
8. Cybercrime is world's most dangerous criminal threat even more severe than any terrorist or nuclear attack if we see total damage by cybercrime in a financial year. (near about > $ 500 billion)

Cybercrime is not only causing damage to defense and security but to anormal person as well as it takes away possibilities of employment. One can fight with thecorporal enemy but not to a virtual enemy, one who only exists in wires, optical fiber, and computer circuits. Awareness, only awareness can solve this problem and we must try to find another safe

alternative of e-governance to stop increasing rate of cybercrime in India and in the world. We can filter internet service for home and school/college use, public and private office and officially sensitive department like defense and home security etc. this classification can help us to stop cybercrime at both national and international level.