# Cyber Crime Issues and Challenges: A Review

**Ajay Kumar Phogat**

*Maharaja Surajmal Institute, New Delhi, India*

---------------------------------------------------------------------***---------------------------------------------------------------------

**Abstract -** Cyber crimes are any crimes that engage a computer and a network. In some cases, the computer may have been used in order to do the crime, and in some cases, the computer may have been the intention of the crime. Computer viruses are computer code that, when opened, put copies of themselves into other computers' hard disk without the users' permission. Developing a computer virus and using it is a cyber crime. The virus may steal disk memory, access personal data, ruin information on the computer or forward information out to the one computer user's personal contacts .The most easy way for a virus to infect a computer is by way of an sending email with virus attachment. An example would be if you get an email with an attachment. You open this attachment, and the virus instantly spreads through your computer system. In some of the cases, if the virus is opened by a computer on a system personal network, such as your place of work, the virus can instantly be spread throughout the network without needing to be sent via email. There are many reasons that a person would create a virus to send out to another computer. It may be to theft information or money, to damage that system or to try the flaws that the other computer system has. In some of the cases these viruses are able to be deleted from the user's computer system, and in some cases they are not removed. Therefore, it is easy for us to understand how these viruses cause financial harm each and every year. The punishment for those who damage or gain unauthorized access to a protected & safe computer can be prison time and the repayment of financial losses too.

***Key Words*:** Cyber Crime, Cyber Space, Cyber Security, Hacking

## 1. INTRODUCTION

The word Cyber crime is increasing day by day. Since the computer is developed and connected to the internet the various types of cyber crime are there in the computer world. The crime in which there is a involvement of any computer is known as cyber crime.

- Consumers are subject to personal identity theft, fraud and inferior simulated or pirated goods.
- Businesses risk losing cognitive property corporate secrets value brought by new innovations, reputation and revenue through espionage and breaches.
- For a nation broader individual losses impact GDP reduce economic growth and innovation and result in a smaller tax base.
- For government's surveillance and cyber attacks threaten national security and diplomatic relations.
- Critical infrastructure that provides water, power, food supply, and healthcare are becoming more attractive career targets for attacks.

### *A.* Cyber crime research

Cyber crime Research is one context where the solution to deal with cyber criminals is generate with the help of cyber law. Investment of time and resources requires advance strategies for research and grow transformative solution to meet critical cyber crimes involving a certain technology.

- The focus of cyber crime research is nowadays to deal with new appear threats and detecting the threats before they effect or cause good amount of damages.
- With attend number of phishing, APTs and Bitnet attacks there is lot to be worked in terms of technological advance and tracking.

### *B.* Secured protocol and algorithms

Research in protocols and algorithms is an important aspect for strengthening the cyber security aspect at a technical level. Protocols and algorithms define the rules for information sharing and processing over online community. In India research has also been undertaken at protocol & algorithm level such as Secure Routing Protocols, Efficient Authentication Protocols, reliability Enhanced Routing Protocol for Wireless Networks, Secure Transmission Control Protocol and Attack Simulation Algorithm etc. These research activities are of great interest to the defense, critical sectors and other sensitive communications in the nation.

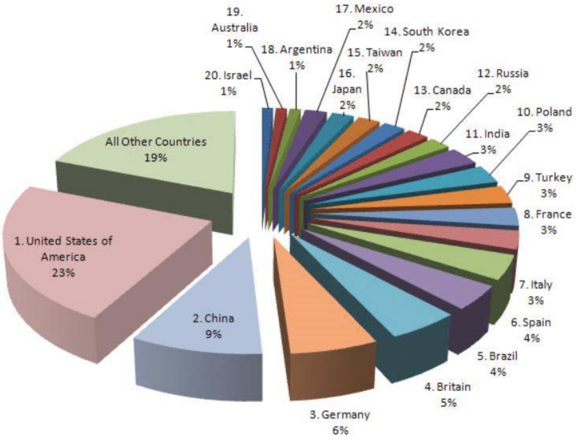

Fig 1. Top 20 countries with cyber crime

### *C.* Research in industry

- Next generation detection technology:

Extend perimeter crime in networks use to detect and await the attacks as early as Possible, but the sheer volume of information in the age of Big Data often makes it tough to detect anomalies that might indicate security issues. Technological research challenges consist of binary solidification, network monitoring, IDS and IPS systems, and attack analysis. Instance to detect and prevent attacks we need techniques and tools to little bit and remove duty from software and monitoring systems to boost and alarm when a system behaves in an odd manner. In order to effectively descry such advanced malware blind of the attack methods being used technology solutions are being developed which use a combination of sophisticated techniques to evaluate advance threats including checking real time emerging campaigns and known new malicious websites that are being detected across organizations and static code division looking for suspicious behavior, obfuscated scripts, malicious code snippets, and modify to other malicious sites. To add solutions based on dynamic analysis by sandboxing the target URL or attachments to simulate a real user on a machine with a goal of observing any changes made to the system are being nudged.

- Command and Control Protection:-

The campaign connected to the Internet can become a target of boot driven attack. Unlike Common attacks targeted Bitnet attacks are very stealthy in nature and are difficult to detect using traditional security solutions. However, despite their close nature, they can cause very high, sometimes irreparable damage to an organization. Research and product development sign at unique “fingerprint” detection of secret C&C traffic which can identify attackers use of accepted applications and Deep discovery custom sandbox analysis can also discover new C&C destinations of intelligent network and all customer crime protection points.

- **Malware and Malicious Infrastructure:-**

Threat of malware will remain critical for the computable future. There is already a pointed trend of increasing malware on social networks in cloud computing and on mobile devices. In terms of research it poses an associative challenge. We need advances in technology for detail in reverse engineering, Bitnet tracking, analysis of criminal framework and classification and accumulate of malware. We need reliable methods to estimate the number of spoil machines and the effectiveness of corrective. Latest promote development of the online Bitnet Extraction and Response System a Bitnet detection and reduction tool which also integrates the online Bitnet extraction capability. Analysis engine and the signature distributor is the technology direction being supported.

### *D.* Recommendations

Despite our efforts cyber crime will continue. However, innovative approaches to this complex problem will enable us to predict appear threats better protect our economies and citizens and minimize the damage from cyber attacks. These advices provide guidance for designing and maintaining enterprise resilience:

- Prefer cyber crime to a strategic role as it impacts the enterprise’s most valued assets.
- Consider cyber crime as a risk stave investment decision not simply a technology purchase.
- Achieve a greater level of protection by sharing data with trusted partners in industry and government, across borders.
- Allow real-time data be the driver for building and convert security strategies.
- Design operational workflows and agenda to support these decisions. Design flexible strong.
- Networks that quickly conform to new threats.
  Create a culture of widespread control for cyber security
- Balance privacy and protection when drafting crime scheme.
- Keep front of mind the privacy rights as well as expectations of protection of those being served by the exploit.
- Keep front of mind the privacy rights as well as expectations of protection of those being served by the exploit.

### *E.* Preventive measures

Creating policy to mitigate cyber threats while preserving privacy and limiting government intercession to a comfortable level is a tricky balancing act. But there are chance to influence future preparedness through forward thinking policy development. Investment in Innovation will be a critical step to maintaining security and ability on a global scale while limiting damage from espionage and other cyber criminal activity. The following areas are important targets for investment as their interrelationship with threat prediction, rapid detection, and damage control makes these especially valuable opportunities.

- Real time- Threat detection and data analysis tools many tools exist today. But their level of sophisticated and widespread adoption must continue to grow to provide more comprehensive protection.
- Big Data- To effectively compile and amount large volumes of data, new technologies and algorithms will be required.
- Visualization tools – Related to big data opportunities are visualization techniques: creative visual presentations of data that quickly differentiate warning indication from normal operating behaviors.
- Emerging technologies- That contribute to resilience more robust protection and adscription of cyber crimes.

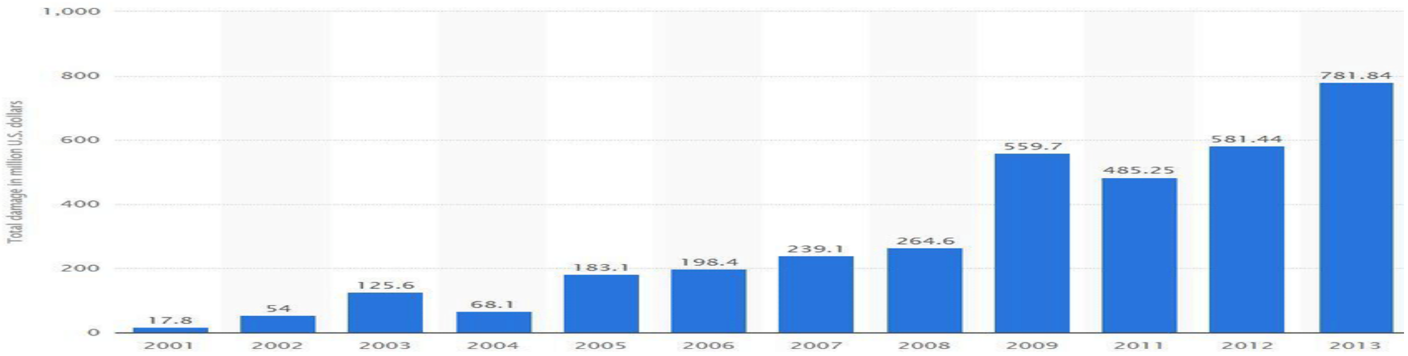

Fig 2. Amount of monetary damage caused by cyber crime from year 2001 to 2013(in million US dollar)

### F. Privacy and government role

Several broader policy issues that govern our collective approach to cyber security have large conclusion for the future:

- The right to privacy by the individual and the activity.
- The act government should play in cyber security.
- Reporting claim for security breaches.
- Lack of consistency in laws and claim between nations and severity of penalties.

These are complex and sometimes doubtable policy issues but purpose established by new policies may have far reaching impact on the level of protection and the approaches we can take to protecting individuals, campaign and state from cyber crime of the future.

### G. The challenge

No matter what strategy is embrace breaches will occur. It is nearly impossible to take advantage of our association without being artist. Technologies such as firewalls, passwords, encryption, physical barriers and authentication. Their value as stand-alone security measures will be of limited use in fighting increasingly artificial, innovative, and well-funded cyber criminals. The emerging challenge is to find more augur methods of identifying threats, relieve their impact and managing an active cyber security operation that will both cooperatively and effectively maintain protection. In accept that challenge. It is important to know that:-

- It is not productive to protect every piece of data and every asset to the same matter.
- A balance between the rights to separation with the need to protect nations.
- Enterprises and individuals from interference must be negotiated.
- Acknowledgment and severe amends for cyber crime must be more uniformly realized within the multi-national communities.
- The challenge is great and desire fresh ways to blend people, processes, technology and shared data to protect societies from appear threats to security.

## 2. CONCLUSIONS

Cyber crime is one of the biggest problem facing by the society in technological world which makes people fearful to perform financial transactions over internet. Recently creation of cybercops, cybercourts and cyberjudges may eventually required to overcome the significant jurisdictional issues.

## REFERENCES

[1]. Etter,B. (2001), The forensic challenges of E-Crime, Current Commentary No. 3 Australasian Centre for Policing Research, Adelaide.

[2]. Etter B. (2002), The challenges of Policing Cyberspace, presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand.

[3]. Eric J. Sinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer a Clara University, Vol 16, Number 2.

[4]. Gengler, B. (2001), Virus Cost hit $20bn, The Australian, 11 September p.36.

[5]. The IT Act 2000.

[6]. Cyber stalking India, www.indianchild.com.

[7]. Cyber crime a new challenge for CBI, www.rediff.com, March 12, 2003 12:27 IST

[8]. Richard Raysman & Peter Brown (1999), Viruses Worms, and other Destructive Forces N. Y. L. J.

[9]. Kabay, M. E. (2000). Studies and Surveys of Computer Crime, Focus.

[10]. KPMG (2000) , E-Commerce and Cyber Crime: New Strategies for Managing the Risks of Exploitation, USA

[11]. Legard, D (2001), Hackers Hit Government Sites, Computer World, Vol 24 No. 26, 29 Jan, p.12. [12]. Russell G. Smith, Peter Grabosky and Grgor Urbas, 0521840473 – Cyber Criminals on Trial, Cambridge University Press.

[13]. Seamus O Clardhuanin (2004), An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Summer 2004, Vol 3, Issue 1

[14]. International crime and Cyber Terrorism, http://www.dfaitmaeci.gc.ca/internationalcrime/cybercrime-en.asp.

[15]K. Chethan, “One cybercrime in India every 10 minutes - Times of India,” The Times of India, 22- Jul-2017.

[16]J. S. Naidu, “10,000 cybercrime cases, only 34 convictions in Maharashtra between 2012 and 2017,” http://www.hindustantimes.com/ 21-Aug- 2017.

[17]V. Nanjappa, “Conviction rate in cyber crime is 0.5 per cent- Here are the reasons,”

[18]A. Seger, “India and the Budapest Convention: Why not?,” ORF.

[19] “7_conv_budapest_en.pdf.”

[20] “T-CY Guidance Note # 3 Transborder access to data (Article 32).”

[21]D. A. Kovacs, “Inda and the Budapest Convention.”

[22] “T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime,” Council of Europe, Strasbourg France, Dec. 2014. [23]K. Seth, “India needs to sign a Cybercrime Convention,” SME Times, 2014.