CYBER CRIME AND SECURITY

A RESEARCH PAPER

PRESENTED BY-

SHILPA YADAV

TANU SHREE

YASHIKA ARORA

RESEARCH PAPER

CYBER CRIME AND SECURITY

Introduction-

The purpose of this paper is *Understanding Cybercrime: Phenomena, Challenges and Legal Response* is to assist everyone in understanding the legal aspects of cyber security and to help harmonize legal frameworks. As such, it aims to help better understand the national and international implications of growing cyber threats, to assess the requirements of existing national, Regional and international instruments, and to assist in establishing a sound legal foundation.

It provides a comprehensive overview of the most relevant topics linked to the legal aspects of Cybercrime and focuses on the demands of developing countries. Due to the transnational dimension of Cybercrime, the legal instruments are the same for developing and developed countries.

Infrastructures and facilities-

The Internet is one of the fastest-growing areas of technical infrastructure development. Today, Information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer

Technology into products that have usually functioned without it, such as cars and buildings. Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs.Although the development of new technologies is focused mainly on meeting consumer demands in western countries, developing countries can also benefit from new technologies.4 With the availability of long-distance wireless communication technologies such as WiMAX5 and computer systems that are now available for less than USD 200, many more people in developing countries should have easier access to the Internet and related products and services.

The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services. E-mails have displaced traditional letter, online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communication and phone services are growing faster than landline communications. The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries.

Advantages and risks-

The introduction of ICTs into many aspects of everyday life has led to the development of the modern Concept of the information society. This development of the information society offers great Opportunities. Unhindered access to information can support democracy, as the flow of information is Taken out of the control of state authorities (as has happened, for example, in Eastern Europe and North Africa).Technical developments have improved daily life – for example, online banking and shopping, the use of mobile data services and voice over Internet protocol (VoIP) telephony are just some examples of how far the integration of ICTs into our daily lives has advanced.

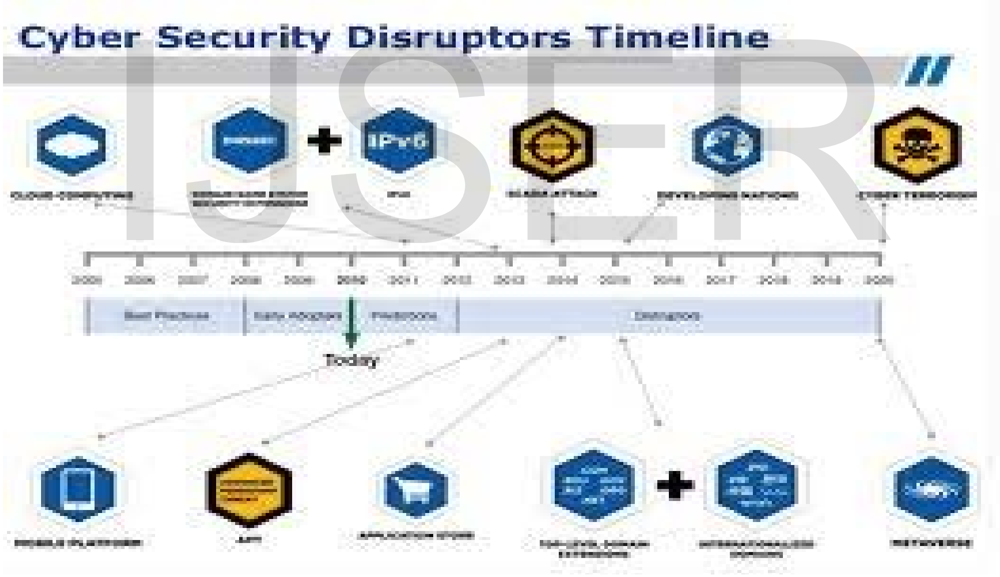
However, the growth of the information society is accompanied by new and serious threats. Essential services such as water and electricity supply now rely on ICTs. Cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of ICTs.23 Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways. Attacks against information infrastructure and Internet services have already taken place. Online fraud and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day. the financial damage caused by cybercrime is reported to be enormous.

Cyber security and cyber crime-

Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cyber security addresses cybercrime as one Major challenge. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. 37 Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being.

Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens.

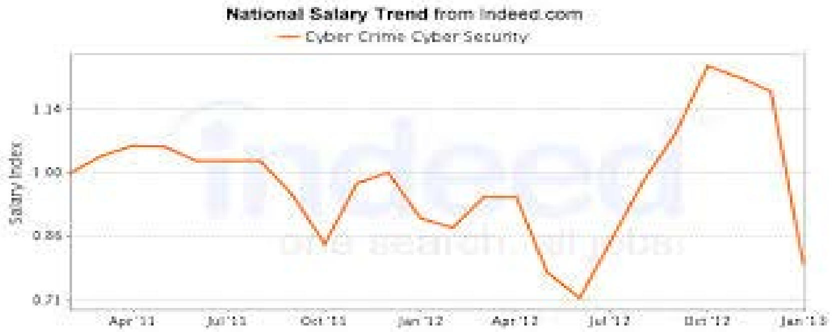
Now the image gives a particular description of the distrupter timeline-



At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach. Cyber security strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime. The development and support of cyber security strategies are a vital element in the fight against cybercrime.

The legal, technical and institutional challenges posed by the issue of cyber security are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.

Crime statistics-



The following numbers have been extracted from national crime statistics. As further discussed below, They are not intended to be representative of either the global development of cybercrime or of the true Extent of cybercrime at the national level, and are thus presented only to provide an insight into country Information.

- The US Internet Complaint Centre reports a 22.3 per cent increase in complaints submitted Relating to cybercrime compared with 2008.
- German Crime Statistics indicate that the overall number of Internet-related crimes increased in 2009 by 23.6 per cent compared with 2008.

It is unclear how representative the statistics are and whether they provide reliable information on the Extent of crime. There are several difficulties associated with determining the global threat of Cybercrime on the basis of crime statistics. Statistical information is useful to draw attention to the continuing and growing importance of the issue, and it is necessary to point out that one of the major challenges related to cybercrime is the lack of reliable information on the extent of the problem, as well as on arrests, prosecutions and convictions.

As already stated, crime statistics often do not list offences separately, and available statistics on the impact of cybercrime are in general unable to provide reliable information about the scale or extent of offences at a level sufficient for policy-makers.

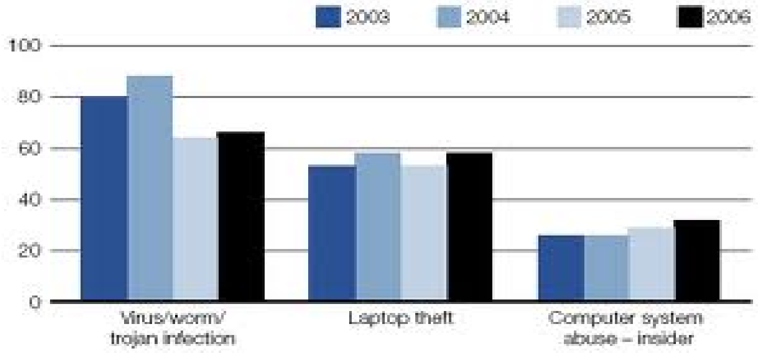
Illegal access-

The offence described as “hacking” refers to unlawful access to a computer system191, one of oldest Computer-related crimes.Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. Famous targets of hacking attacks include the US National Aeronautics and Space Administration (NASA), the US Air Force, the Pentagon, Yahoo, Google, eBay and the German Government.

Examples of hacking offences include breaking the password of password-protected websites and Circumventing password protection on a computer system. But acts related to the term “hacking” also Include preparatory acts such as the use of faulty hardware or software implementation to illegally obtain a password to enter a computer system, setting up “spoofing” websites to make users disclose their Passwords and installing hardware and software-based key logging methods (e.g. “key loggers”) that Record every keystroke – and consequently any passwords used on the computer and/or device.

Many analysts recognize a rising number of attempts to illegally access computer systems, with over 250 million incidents recorded worldwide during the month of August 2007 alone. Three main factors have supported the increasing number of hacking attacks: inadequate and incomplete protection of computer systems, development of software tools that automate the attacks, and the growing role of private computers as a target of hacking attacks.

Statistics of the cyber crime-



Inadequate and incomplete protection of computer systems

Hundreds of millions of computers are connected to the Internet, and many computer systems are Without adequate protection in place to prevent illegal access. Analysis carried out by the University of Maryland suggests that an unprotected computer system that is connected to the Internet is likely to Experience attack within less than a minute. The installation of protective measures can lower the risk, but successful attacks against well-protected computer systems prove that technical protection measures can never completely stop attacks.

Development of software tools that automate the attacks

Recently, software tools are being used to automate attacks. With the help of software and preinstalled attacks, a single offender can attack thousands of computer systems in a single day using one computer. If the offender has access to more computers – e.g. through a botnet – he/she can increase the scale still further. Since most of these software tools use preset methods of attacks, not all attacks prove successful.

Users that update their operating systems and software applications on a regular basis reduce their risk of falling victim to these broad-based attacks, as the companies developing protection software analyse attack tools and prepare for the standardized hacking attacks.
High-profile attacks are often based on individually-designed attacks.

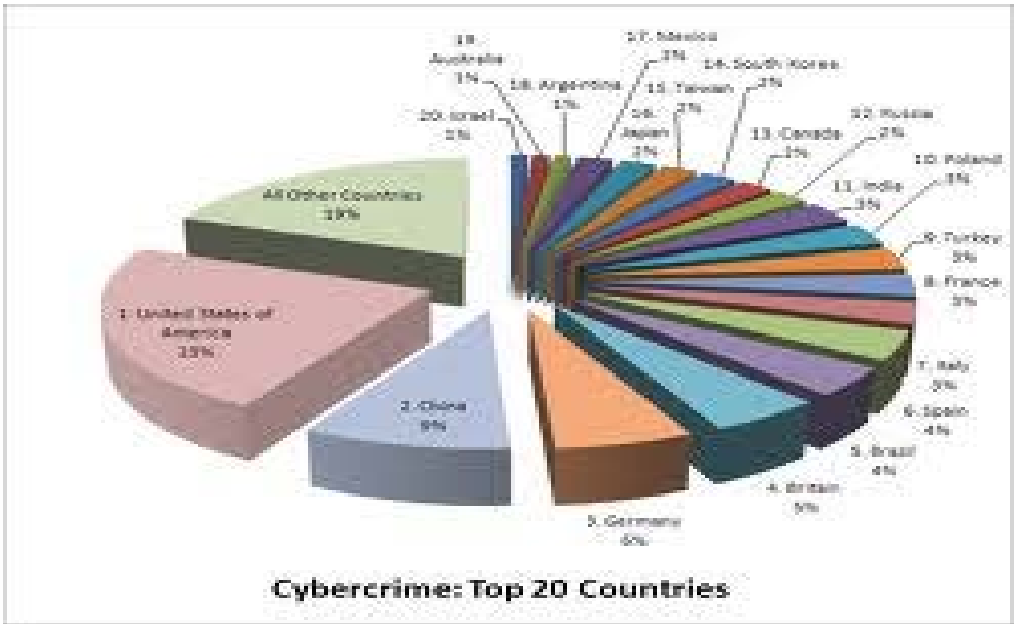
Illegal data acquisition (data espionage)

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world. The Internet is increasingly used to obtain trade secrets. The value of sensitive information and the ability to access it remotely makes data espionage highly interesting. In the 1980s, a number of German hackers succeeded in entering US government and military computer systems, obtaining secret information and selling this information to agents from a different country.

Illegal interception-

Offenders can intercept communications between users(such as e-mails) or other forms of data transfers (when users upload data onto webservers or access web-based external storage media) in order to record the information exchanged. In this context, offenders can in general target any communication infrastructure (e.g. fixed lines or wireless) and any Internet service (e.g. e-mail, chat or VoIP communications).

Top countries having threat of cyber crime-

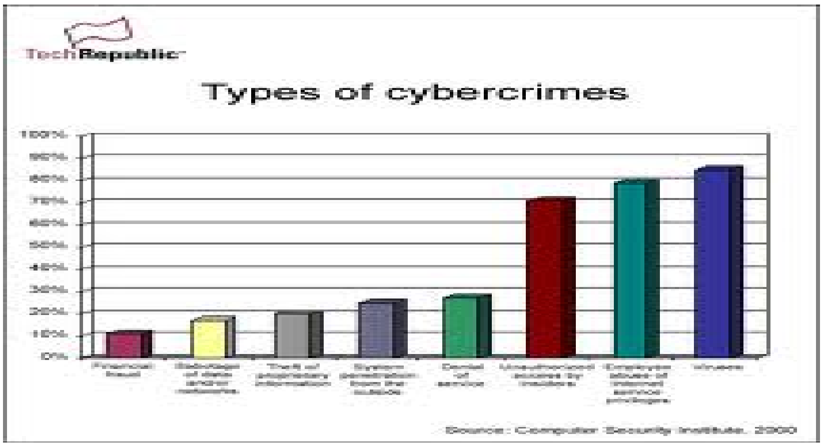


Various types of cyber crimes-

There are several types of cyber crimes that are occurring in the networking world some of these are as written below-

1. Financial fraud
2. Sabotage of data and other networks
3. Theft of proprietery information
4. System penetration from outside
5. Denial of service
6. Unauthorised access by insiders
7. Employee use of internet service privileges
8. Viruses

Here the picture depicts the type of crimes and the threat percentage of these crimes-



Anti-cybercrime strategies-

Cybersecurity plays an important role in the ongoing development ofinformation technology, as well as Internet services. Making the Internet safer (and protecting Internetusers) has become integral to the development of new services as well as governmental policy.

Cybersecurity strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime.

An anti-cybercrime strategy should be an integral element of a cybersecurity strategy.

The ITU Global Cybersecurity Agenda, as a global framework for dialogue and international cooperation to coordinatethe international response to the growing challenges to cybersecurity and to enhance confidence andsecurity in the information society, builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address these related challenges.

Conclusions-

The cyber crime as a whole refers to Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation’s security and financial health. Issues surrounding this type of crime have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

A computer can be a source of evidence. Even when a computer is not directly used for criminal purposes, may contain records of value to criminal investigators.so the network must be secure as no one can access the information of the computer.

References-

1. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

2. Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, ABC-CLIO, 2010.

Also includes the statistics from the net search and many other sites.