

INTRODUCTION TO CYBER SPACE 1.1 INTRODUCTION Internet is among the most important inventions of the 21st century which have affected our life. Today internet have crosses every barrier and have changed the way we use to talk, play games, work, shop, make friends, listen music, see movies, order food, pay bill, greet your friend on his birthday/ anniversary, etc. You name it, and we have an app in place for that. It has facilitated our life by making it comfortable. Gone are the days when we have to stand in a long queue for paying our telephone and electricity bills. Now we can pay it at a click of a button from our home or office. The technology have reached to an extent that we don't even require a computer for using internet. Now we have internet enabled smartphone, palmtops, etc. through which we can remain connected to our friends, family and office 24x7. Not only internet has simplified our life but also it has brought many things within the reach of the middle class by making them cost effective. It was not long back, while making an ISD or even a STD call, the eyes were stricken on the pulse meter. The calls were very costly. ISD and STD were used to pass on urgent messages only and the rest of the routine communication was done using letters since it was a relatively very cheap. Now internet have made it possible to not only talk but use video conference using popular applications like skype, gtalk etc. at a very low price to a level where a one hour video chat using internet is cheaper than the cost of sending a one page document from Delhi to Bangalore using speedpost or courier service. Not only this, internet has changed the use of the typical devices that were used by us. Television can be used not only for watching popular tv shows and movies but can be used for calling/ video chatting with friend using internet. Mobile phone is not only used for making a call but viewing a latest movie. We can remain connected to everyone, no matter what our location is. Working parents from office can keep eye on their children at home and help them in their homework. A businessman can keep eye on his staff, office, shop, etc with a click of a button. It has facilitated our life in more than one way. Have you ever wondered from where this internet came? Let us discuss the brief history of internet and learn how this internet was invented and how it evolved to an extent that now we cannot think of our lives without it.

1.1.1 History of Internet

I don't know what the cold war between USA and Russia gave to the world, but defiantly the internet is one of those very useful inventions whose foundation was laid during cold war 9 days.

Russia launched the world's first satellite, SPUTNIK into the space on 4th October, 1957. This was clearly the victory of Russia over the cyber space and as a counter step, Advanced Research Projects Agency, the research arm of Department of Defence, United States, declared the launch of ARPANET (Advanced Research Projects Agency NETWORK) in early 1960's. This was an experimental network and was designed to keep the computers connected to this network to communicate with each other even if any of the node, due to the bomb attack, fails to respond. The first message was sent over the ARPANET, a packet switching network, by Leonard Kleinrock's laboratory at University of California, Los Angeles (UCLA). You will be surprised to know that the first message that was sent over internet was "LO". Actually they intended to send word "LOGIN" and only the first two letters reached its destination at second network node at Stanford Research Institute (SRI) and before the last three letters could reach the destination the network was down due to glitch. Soon the error was fixed and the message was resent and it was The major task that ARPANET had to play is to develop rules for communication i.e. protocols for communicating over ARPANET. The ARPANET in particular led to the development of protocols for internetworking, in which multiple separate networks could be joined into a network of networks. It resulted in the development of TCP/IP protocol suite, which specifies the rules for joining and communicating over ARPANET. Soon after, in 1986 NSF (National Science Foundation) backbone was created to connect five US universities' computing centres were connected to form NSFnet. The participating Universities were:

- Princeton University -- John von Neumann National Supercomputer Center, JvNC
- Cornell University -- Cornell Theory Center, CTC
- University of Illinois at Urbana-Champaign -- National Center for Supercomputing Applications, NCSA
- Carnegie Mellon University -- Pittsburgh Supercomputer Center, PSC
- General Atomics -- San Diego Supercomputer Center, SDSC

NSFnet, the successor of ARPANet, became popular by 1990 and ARPANET was decommissioned. There were many parallel networks developed by other Universities and other countries like United Kingdom. In 1965, National Physical Laboratory (NPL) proposed a packet switching network. Michigan Educational Research Information Triad formed MERIT network in 1966 which was funded and supported by State of Michigan and the 10 National Science Foundation (NSF). France also developed a packet switching network, known as

CYCLADES in 1973. Now there were many parallel systems working on different protocols and the scientist were looking for some common standard so that the networks could be interconnected. In 1978, TCP/IP protocol suits were ready and by 1983, the TCP/IP protocol were adopted by ARPANET. In 1981, the integration of two large network took place. NSF developed Computer Science Network(CSNET) and was connected to ARPANET using TCP/IP protocol suite. Now the network was not only popular among the research community but the private played also took interest in the network. Initially NSF supported speed of 56 kbit/s. It was upgraded to 1.5 Mbit/s in 1988 to facilitate the growth of network by involving merit network, IBM, MCA and the state of Michigan. After the corporate took realized the strength and merit of this network, they participated in the development of the network to reap its benefits. By late 1980s many Internet Service Providers(ISPs) emerged to provide the backbone for carrying the network traffic. By 1991, NSFNET was expanded and was upgraded to 45Mbit/s. Many commercial ISPs provided backbone service and was popular among the corporate. To facilitate the commercial use of the network, NSFNET was decommissioned in 1995 and now the Internet could carry commercial traffic. Now more and more Universities and research centres throughout the world connected to it. Now this network was very popular among the research community and in 1991 National Research and Education Network (NREN) was founded and the World Wide Web was released. Initially the role of internet was only limited to file transfer. The credit of internet what we see it today goes to Tim Berners-Lee who introduced www. With the advent of www, there was a transformation on how the network was used. Now this web of information can be used to retrieve any information available over the internet. Software called, browser was developed to browse the internet. It was developed by researchers at University of Illinois in 1992 and named as Mosaic. This browser enables to browse the internet the way we browse it today.

1.1.1.1 Internet Addresses

With so many devices connected to the internet, we require some mechanism to uniquely identify every device that is connected to the internet. Also we require some centralized system which takes care of this mechanism so that the signs which are used to identify each device are not duplicate; else the whole purpose is defeated. To take care of this, we have a centralized authority known as Internet Assigned Numbers Authority (IANA), which is

responsible for assigning a unique number known as IP(Internet Protocol) address. An IP address is a 32-bit binary number which is divided into four octets and each octet consists of 8 binary digits and these octet are separated by a dot(.). An example of an IP address is 11110110.01011010.10011100.1111100

Each 8-bits in an octet can have two binary values i.e. 0 and 1. Therefore, each octet can have minimum value 0. i.e. 00000000 to maximum value 255 i.e. 11111111 and in total have $2^8 = 256$ different combinations. Again to remember this 32-bit address in binary is bit difficult, so for the better understanding of the human being, it is expressed in a decimal format. But this decimal format is for human understanding only and the computer understands it in binary format only. In decimal, the above IP address is expressed as 123.45.78.125

These octets are used to create and separate different classes. An IP address consists of two parts viz. Network and Host. Network part identifies the network different network and the host part identifies a device of a particular network. This address uniquely identifies a devices connected to the internet similar to the postal system where we identify any house by fist identifying the county, then state, district, post office, cluster/block and finally the house number. These IP addresses are classified into five categories based on the availability of IP range. These categories/classes are:

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

IANA decentralises that task of assigning the IP addresses by allocating the large chunk of IP addresses to five Regional Internet Registries (RIRs), which are further responsible to 12 allocate the IP addresses in their zone. These RIRs along with their area of operations are listed below:

- APNIC- This RIR is responsible for serving the Asia Pacific region
- AfriNIC- This RIR is responsible for serving the African region
- ARIN- This RIR is responsible for serving North America and several Caribbean and North Atlantic islands
- LACNIC- This RIR is responsible for serving Latin America and the Caribbean, and
- RIPE NCC- This RIR is responsible for serving Europe, the Middle East, and parts of Central Asia

For

liaison and coordinating between these five RIRs, there is an organization called Number Resource Organization(NRO). These organizations are 1.1.1.2

DNS Whenever we browse any website in the internet, we type name something like www.uou.ac.in and we rarely deal with IP address like 104.28.2.92 but the fact is even if we type http:\\ 104.28.2.92 in the URL, it will land us to the same webpage. The fact is we are very comfortable using and remembering the names instead of a number. Moreover, these IP address changes over time and some of the sites have multiple IP address. Also, the transfer of the data over internet is only possible using IP addresses because the routing of the packet of data sent over internet is done using IP address. There is a server called Domain Name System(DNS) which take cares of this translation job to simplify and to save us from remembering these changing IP address numbers, the DNS. Whenever you type an address like http:\\www.uou.ac.in, there is a process called DNS name resolution, takes place in the background. The computer keeps the track of recently visited sites and locally maintains a database in DNS cache. In case, the IP address of the site you have requested for is not found in the DNS cache of your local computer, then the next probable place to find it is DNS server of your Internet Service Provider(ISP). These DNS servers of ISP also maintain the cache of the recently visited pages. Just in case, the information is not found here also, the DNS server of the ISP forward the query to the root nameservers. The root name servers publish the root zone file to other DNS servers and clients on the Internet. The root zone file describes where the authoritative servers for the DNS top-level domains (TLD) are located. There are currently 13 rootname servers. They are: → A - VeriSign Global Registry Services 13 → B - University of Southern California - Information Sciences Institute → C - Cogent Communications → D - University of Maryland → E - NASA Ames Research Center → F - Internet Systems Consortium, Inc. → G - U.S. DOD Network Information Center → H - U.S. Army Research Lab → I - Autonomica/NORDUnet → J - VeriSign Global Registry Services → K - RIPE NCC → L - ICANN → M - WIDE Project These root nameservers directs the query to the appropriate Top-Level Domain(TLD) nameservers by reading the last part of the URL first. In our example the url was http:\\www.uou.ac.in. The last part is .in. Some of the examples of TLD name servers are .com, .biz, .org, .us, .in, etc. These TLD nameservers acts as a switchboard and direct the query to the appropriate

authoritative nameserver maintained by each domain. These authoritative nameserver maintains DNS records along with other useful information. This address record is returned back to the requesting host computer via TLD nameservers, nameservers, ISP's DNS server. These intermediary server keeps the record of this IP address in their DNS cache, so that if the same request is encountered again, they don't have to go through this process again. If the same URL is requested again, the DNS cache of the local host computer will return the IP address of the URL.

1.1.1.3 Internet Infrastructure

Internet, as the name suggests, is a network of networks i.e. it is a collection of several small, medium and large networks. This clearly indicates one fact, nobody is a single owner of the internet and it is one of the proven examples of collaborative success. Now you must be surprised how such a large network which is spread across the continents can run without any problem. Yes it is correct that to monitor such a large network, we require an international body which can frame the rules, regulations and protocols to join and use this network. Therefore, an international organization, known as "The Internet Society" was formed in 1992 to take care of such issues.

14 Let us now discuss, how this internet works?

How the email you sent to your friend is received by your friend's computer located at another country/continent. When you are working on your laptop/desktop in your home without connecting to the internet, your computer is a standalone system. But, whenever you connect to the internet by dialling to your Internet Service Provider (ISP) using your modem, you become the part of the network. The ISP is the link between the internet backbone, through which the entire data route, and the user. The ISP connects to the internet backbone at Network Access Points (NAP). These NAPs are provided by the large telecommunication companies at various regions. These large telecommunication companies connect the countries and the continents by building and maintaining the large backbone infrastructure to route data from NAP to NAP. ISPs are connected to this backbone at NAP and are responsible to build and manage the network locally. So when you dial internet through modem, you first become part of the local ISP, which in turn connects to the internet backbone through NAP. The data is routed through this backbone and sent to the destination NAP, where the ISP of your friend's network is located. As soon as your friend dials his modem to connect to the internet, the data is delivered to your friend's computer.

1.1.1.4 World Wide

Web Sometimes we interchangeably use the term internet and world wide web or simply the web, as it is popularly known as. But web is only one of the several the utilities that internet provides. Some of the popular service that internet provides other than web is e-mail, usenet, messaging service, FTP, etc. The web use HTTP protocol to communicate over internet and to exchange information. The web was developed at CERN (European de Reserches Nucleaires), Switzerland) by a UK scientist Tim Berners-Lee in 1989. It consists of all the public web sites and all the devices that access the web content. WWW is an information sharing model which is developed to exchange information over the internet. There are plenty of public websites, which is a collection of web pages, available over the internet. These webpages contain plenty of information in a form of text, videos, audio and picture format. These web pages are access using a application software called a web browser. Some of the examples of the popular web browser are: Internet explorer, Chrome, Safari, Firefox, etc. So this was a little indroduction about internet and how it functions. Now let us discuss about cyber crime.

1.2 INTRODUCTION TO CYBER CRIME

The internet was born around 1960"s where its access was limited to few scientist, researchers and the defence only. Internet user base have evolved expontinanlty. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure. Around 1980"s the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus. Till then the effect was not so widesread beacouse internet was only confined to defence setups, large international companies and research communities. In 1996, when internet was launched for the public, it immeditly became populer among the masses and they slowly became dependent on it to an extent that it have changed their lifestyle. The GUIs were written so well that the user don"t have to bother how the internet was functioning. They have to simply make few click over the hyber links or type the desired information at the desired place without bothering where this data is stored and how it is sent over the internet or wether the data can accessed by another person who is conneted to the internet or wether the data packet sent over the internet can be snoofed and tempered. The focus of the computer crime shifted from marely damaging the computer or destroying or manipulating data for personal benefit to financial crime. These computer attacks are incresing at a rapid

pase. Every second around 25 computer became victim to cyber attack and around 800 million individuals are effected by it till 2013. CERT-India have reported around 308371 Indian websites to be hacked between 2011-2013. It is also estimated that around \$160 million are lost per year due to cyber crime. This figure is very conservative as most of the cases are never reported. Accoring to the 2013-14 report of the standing committee on Information Technology to the 15th Lok Sabha by ministry of communication and information technology, India is a third largest number do Intrnet users throughout the world with an estimated 100 million internet users as on June, 2011 and the numbers are growing rapidly. There are around 22 million broadband connections in India till date operated by around 134 major Internet Service Providers(ISPs). Before discussing the matter further, let us know what the cyber crime is? The term cyber crime is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal acitivity. It is often 16 committed by the people of destructive and criminal mindset either for revenge, greed or adventure.