Chapter III
INFRASTRUCTURE AND STANDARDISATION

3.1 Infrastructure Essentials:
At first we discuss most basic entities or issues required for the existence of the internet and the World Wide Web. These issues are often collected together to form three relevant layers, also popularly know as three stage model of infrastructural requirements. The classification is as follows:

   a. The telecommunications infrastructure, through which all internet traffic flows.
   b. The infrastructure that makes the Internet work ‘TCP/IP’, ‘DNS’ and ‘SSL’
   c. The content and applications standards HTML, XML

3.1.1 Transmission Control Protocol and Internet protocol (TCP/IP):
It is the Internet’s main technical standard, specifying how data is moved through. A less used name for it is the Internet Protocol Suite, which is the phrase used in official Internet standards documents. TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved. From lowest to highest, the layers are the link layer, containing communication technologies for a single network segment (link), the internet layer, connecting independent networks, thus establishing internetworking, the transport layer handling host-to-host communication, and the application layer, which contains all protocols for specific data communications services on a process-to-process level.¹
It is based on three principles: packet-switching, end-to-end networking, and robustness.

*Packet switching* is the method used to transmit data over the Internet. All the data sent from one computer is split into packets that travel over the Internet and are then reassembled when they reach the destination computer.

*End-to-end networking* puts all sophistication, intelligence, and innovation at the edges of a network. This principle has made all the Internet-related innovations possible. The network between the end-points is neutral and does not prevent development and creativity at the endpoints. This means that applications that run over the Internet can be designed without requiring permission from network operators or any other parties.

The end to end arguments suggest that specific application-level functions usually cannot, and preferably should not, be built into the lower levels of the system—the core of the network. The reason why was stated as follows in the original paper: *The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system.*

*Robustness* is achieved through dynamic routing. Initially, the Internet’s predecessor, ARPANET, introduced dynamic routing in order to develop robust defence networks capable of surviving a potential nuclear attack. Dynamic routing was used to interconnect a diverse set of networks.

The Internet protocol suite historically resulted from research and development conducted by the Defence Advanced Research Projects Agency (DARPA) in the late 1960s. After initiating ARPANET in 1969,
DARPA started work on a number of other data transmission technologies. In 1972, Robert E. Kahn joined the DARPA Information Processing Technology Office, where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the value of being able to communicate across both. In 1973, Vinton Cerf, the developer of the existing ARPANET Network Control Program (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next protocol generation for the ARPANET.

The main design goal of TCP/IP was to build an interconnection of networks, referred to as an internet-work, or internet, that provided universal communication services over heterogeneous physical networks. The clear benefit of such an internet-work is the enabling of communication between hosts on different networks, perhaps separated by a large geographical area.4

Internet Governance related to TCP/IP has two important aspects:

a) The introduction of new standards: TCP/IP standards are set and carefully guarded by the Internet Engineering Task Force (IETF). Any changes to TCP/IP require extensive prior discussion and proof that they are an effective solution.

b) The distribution of IP Address: An Internet Protocol address number assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.
IP numbers are unique numeric addresses that all computers connected to the Internet must have. Two computers connected to the Internet cannot have the same IP number. This makes IP numbers a very scarce resource. The system for the distribution of IP numbers is hierarchically organised. At the top is IANA which distributes blocks of IP numbers to the five regional Internet registries (RIRs). RIRs distribute IP numbers to the local Internet registries (LIRs) and national Internet registries (NIRs), which in turn distribute IP numbers to smaller ISPs, companies, and individuals further down.\(^5\)

One of the important governance issues is the increasing demand of large IP numbers due to internet enabled devices like mobile phones, personal organisers, game consoles, and home appliances. The current protocol IPv4 can support only about 4.2 billion addresses which is very less compared the current and future IP demands. To compensate this acute shortage and to further promote the development, the technical community has taken then following three steps.

1. Introduce a process known as “Network Address Translation” (NAT), which allows for the use of private addresses. Under NAT, individual computers on a single private network (for example, within a company or university) use non-unique private addresses that are translated into public, unique IP addresses as they leave the private network boundary.

2. Address the wasteful address allocation algorithms used by the RIRs by introducing Classless Inter-Domain Routing (CIDR).

3. The technical community has developed a new protocol known as IPv6. This protocol, which would allow for some \((3.4 \times 10^{38})\) addresses, essentially solves the shortage problem. IPv6 also introduces
a range of additional features not currently supported in IPv4, including better security, and the ability to differentiate between different streams of packets (e.g. voice and data).\textsuperscript{6}

One of the main challenges facing the deployment of IPv6 is the lack of backward compatibility between IPv6 and IPv4. Networks using IPv6 cannot communicate directly to those, still dominant today, using IPv4. Since it is very likely that networks using IPv4 and IPv6 will coexist during the coming period, it is important to ensure that new – IPv6-based – networks do not remain isolated.

A technical solution will involve special tunnelling between the two types of networks, which will cause more complex routing on the Internet and a few other similar problems. Excluding the problems associated with transition from IPv4 to IPv6, the policy framework for IPv6 distribution will require a proper distribution of IP numbers, demanding the introduction of open and competitive mechanisms to address the needs of end-users in the most optimal way. Even with the introduction of IPv6 an ‘artificial’ scarcity of IP numbers could still arise, if those responsible for allocating them at local level, such as ISPs, choose to misuse their power and link such allocation to, for example, the purchase of other services, thus affecting the availability and price of IP numbers.\textsuperscript{7}

\textbf{3.1.2 Domain name System (DNS):}

Short for Domain Name System, an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. Every time you use a domain name, a DNS service translates the name into the corresponding IP address. For example, the
domain name www.example.com might translate to 198.105.232.4 in (IPv4) and 2001:500:88:200::10 in (IPv6).

The Internet had eight top-level domain names till 2000: .arpa, .com, .net, .org, .int, .edu, .gov and .mil. These domains are called generic top-level domains, or gTLDs. As the Internet grew, there were increasing calls for more top-level domain names to be added. ICANN announced seven new gTLDs: .aero, .biz, .coop, .info, .museum, .name, and .pro. Another series of new gTLDs have also been announced but still few of them are not active. DNS also consists of a different set of names called as country code top-level domains or ccTLDs, these two letter codes such as .in(India), .au(Australia), .fr(France) were created for country wise representation. The DNS consists of root servers, top-level domain (TLD) servers, and a large number of DNS servers located around the world.8

One of the primary functions of DNS management is the protection of trademark and dispute resolution. The loose methods of allocating domain names in early days resulted in cyber-squatting (practice of registering domain names that could be resold later). The Uniform Dispute Resolution Policy (UDRP) developed by ICANN and the World Intellectual Property Organisation (WIPO) provides mechanisms that have significantly reduced cyber-squatting.

Governance related issues of DNS can be listed as follows.
A. New generic domain names: Though creating TLDs has no technical complexity but it is a slow and widely debated process. After long discussions ICANN began implementing of new gTLDs not before 2012.
New program permits any organisation to apply and run new gTLD registry, including non-Latin language scripts.

B. Managing Country domains: Three sub-issues are to be taken care of.
   a. which country codes should be registered when dealing with countries and entities with unclear or contested international status.
   b. who should manage ccTLD, because it is considered to be a national resource.
   c. Initial refusal of many country domain operators to become part of the ICANN system. As ICANN did not took country domain operators in full confidence, regional level domain operators are in existence. (Europe – CENTR, Africa – AFTLD, Asia – APTLD, North America – NATLD, and South America – LACTLD). At global level, the main forum is the World Wide Alliance of Top Level Domains.

C. English remained a dominant language in the overall development process of internet. Being a global communication medium it has even attracted many non-English speakers in the governance process. Internet infrastructure and services could have a greater impact on the overall development, if multilingual features were incorporated.

D. Multilingual domain names/Internationalised domain names: After a long testing and political uncertainty, in May 2010 ICANN started approving TLDs in scripts other then English like Chinese, Arabic and Cyrillic. One of the main successes of the internet governance process is the introduction of Internationalised domain names (IDNs). The only
problem with IDN is the threat of Phishing because the character set used by ISO 10646 some times look similar in appearance.\textsuperscript{9}

E. DNSSEC: The original design of the Domain Name System (DNS) did not include security; instead it was designed to be a scalable distributed system. The Domain Name System Security Extensions (DNSSEC) attempts to add security, while maintaining backwards compatibility. DNSSEC applies well-established public key cryptography to ensure data integrity and origin authenticity in the DNS system.\textsuperscript{10}

F. Root Servers: At the top of the DNS hierarchical structure, root servers attract a lot of attention. They are a part of most policy and academic debates on Internet governance issues. There are 13 root servers distributed around the world, 10 in the USA and one each in Sweden, the Netherlands, and Japan; of the 10 in the USA, several are operated by US government agencies. If one server crashes, the remaining 12 would continue to function.

The 13 root servers are managed by different organisations: academic/public institutions (7), commercial companies (3), and government institutions (3). Institutions managing root servers receive a root zone file proposed by IANA (ICANN) and approved by the US government (Department of Commerce). Once the content is approved by the Department of Commerce, it is entered into the master root server operated by VeriSign under contract to the Department.
3.1.3 Secure socket layer (SS)

SSL (Secure Sockets Layer) is the standard security technology for establishing a secure link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http.

Browsers provide a key indicator to know that we are currently protected by an SSL encrypted session the lock icon in the lower right-hand corner, clicking on the lock icon displays your SSL Certificate and the details about it. SSL Certificate will contain your domain name, your company name, your address, your city, your state and your country. It will also contain the expiration date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate.

Authenticating the server is a critical part of SSL connection establishment. This authentication takes place during the SSL handshake, when the server presents its public-key certificate. In order for the SSL connection to be secure, the client must carefully verify that the certificate has been issued by a valid certificate authority, has not expired or been revoked, the names listed in the certificate matches the name of the domain that the client is connecting to, and perform several other checks.\textsuperscript{11}
3.2 Managing content and applications:
Earlier content managers could handled only text and photos, but newer internet applications required more sophisticated technologies for managing databases, video, and animation. Such a variety of applications required considerable standardisation efforts in order to ensure that internet content could be properly viewed by the majority of Internet browsers. We discuss few commonly available content managers and applications below.

3.2.1 Hyper Text Markup Language (HTML):
It is the main language for creating web pages that can be displayed in a web browser. The purpose of a web browser is to read HTML documents and convert them into visible or audible web pages. Without displaying HTML tags the browser uses the tags to interpret the content of the page. An HTML element acts as the building blocks of all websites. Using HTML, images and objects can be embedded and used to create interactive forms. It provides a means to create structured documents by applying structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. It can embed scripts written in languages such as JavaScript which affect the behaviour of HTML web pages.
To define the appearance and layout of text and other material Web browsers can also refer to Cascading Style Sheets (CSS). W3C maintains both the HTML and the CSS standards and encourages the use of CSS over explicit presentational HTML.\textsuperscript{12}

In the last part of year 1990 Berners-Lee proposed an Internet-based hypertext system called as HTML and wrote the browser and server software. In 1991 the first publicly available description of HTML was a document called "HTML Tags". It describes 18 elements comprising the
initial, relatively simple design of HTML. Basic characteristics for every item of HTML are defined in the browser, and these characteristics can be altered or enhanced by the web page designer’s additional use of CSS. It consists of several key components like, elements and their attributes, character-based data types, character references and entity references. Document type declaration is also an important component which triggers standards mode rendering. These documents can be delivered by the same means as any other computer file. However, they are most often delivered either by HTTP from a web server or by email. Commonly filename extension for files containing HTML is .html

Three Rules from Tim Berners-Lee: If the past was document sharing, the future is data sharing. Berners-Lee says now, “I want you to put your data on the Web.” But how should we go about that? To answer that question, he provides three points of instruction. One, a URL should point to the data. Two, anyone accessing the URL should get data back. Three, relationships in the data should point to additional URLs with data.13

3.2.2 Extensible Markup Language (XML):
XML is a markup language for documents containing structured information. A markup language is a mechanism to identify structures in a document. The XML specification defines a standard way to add markup to documents. It is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere. XML can be used by any individual or group of individuals or companies that wants to share information in a consistent way. XML defines a set of rules for encoding documents in a format that is both human and machine readable.
XML was developed by an XML Working Group formed under the sponsorship of the World Wide Web Consortium (W3C) in 1996. It was chaired by Jon Bosak of Sun Microsystems with the active participation of an XML Special Interest Group.\textsuperscript{14}

Few of the design goals for XML were as follows:

1. XML shall be directly usable over the Internet.
2. XML shall support a wide variety of applications.
3. XML shall be compatible with SGML.
4. It shall be easy to write programs which process XML documents.
5. XML documents should be human-legible and reasonably clear.
6. XML documents shall be easy to create.

XML has two current versions, the first (XML 1.0) was initially defined in 1998. It has undergone minor revisions since then, without being given a new version number, and is currently in its fifth edition, as published in 2008. It is widely implemented and still recommended for general use. XML is "extensible" because, unlike HTML, the markup symbols are unlimited and self-defining.

Another source of XML's unifying strength is its reliance on a new standard called Unicode, a character-encoding system that supports intermingling of text in all the world's major languages. In HTML, as in most word processors, a document is generally in one particular language, whether that be English or Japanese or Arabic. If your software cannot read the characters of that language, then you cannot use the document. The situation can be even worse: software made for use in Taiwan often cannot read mainland-Chinese texts because of incompatible encodings. But
software that reads XML properly can deal with any combination of any of these character sets. Thus, XML enables exchange of information not only between different computer systems but also across national and cultural boundaries.¹⁵

3.3 Security and stability Essentials:
The Internet was initially used by a closed circle of mainly academics without security concerns, but due to rapid expansion of the Internet users technology became both enabling and threatening. What can be used to the benefit of society can also be used to harm. For a safe and secure use of internet, suitable security measures are to be adopted.

3.3.1 Data Interception:¹⁶
User’s Internet traffic can be intercepted from the computers sharing same LAN (local area network) or wireless network with the computer being monitored. Data interception is the danger you should count with. How can we protect ourselves from data interception? To find the proper solution we should understand first how the data interception could be performed.

Internet is build as a hierarchy system. End users are connected to the ISP network through the DSL/cable connections or dialup, ISPs networks are connected to a few bigger, national wide ISPs, and big ISPs are connected between themselves. There are special computers to find the proper path for data packets travelling to the destination, ISP gateways or routers that examine each packet passing through them and transferring it to the next gateway until the packet reaches its destination. The path between the source network and the destination network is called “route”. Routes (paths between networks) are being chosen depending on the network load, link
availability, etc. and change frequently, sometimes a few times a day. Usually data packets are travelling to the destination server through dozen of different networks and gateways.

After data packets are leaving your PC they are passed to the ISP gateway. ISP gateway, which has multiple connections to the bigger ISP networks, will examine destination IP address, choose proper “next hop” gateway and then forward packet to this gateway. New gateway will perform the same procedure, and so on.

So where is a weak point in this chain? There is a single point where all your data is passed: your ISP gateway. After the packet leaves your ISP network it is almost impossible to predict its route, since it will depend on the destination. Even if the destination is same, the routes change, today it is one route, and tomorrow it will be some other. To monitor somebody’s Internet activities the interested party should monitor the ISP traffic, the single point where all this traffic is passed through. To protect your data from the interception you should use traffic encryption. This will guarantee that neither ISP staff nor government authorities can intercept your data.

3.3.2 Data Interference:
The damaging, deletion, alternation or unauthorized suppression of computer data is considered as examples of data interference, when this offence is committed against the computer data of the military, public order, civil protection, health care or any other computer data of public importance.
3.3.3 Data corruption:

When Computer data becomes unusable, unreadable or in some other way inaccessible to a user or application due to errors that occur during writing, reading, storage, transmission, then it is referred to as data corruption. Some common reasons for data corruption and loss include:

a. Power failures or other power-related problems.

b. Improper shutdowns, such as caused by power failures or performing an emergency restart.

c. Hardware problems or failures, including hard drive failures, bad sectors, bad RAM, and the like.

d. Failure to eject external hard drives and related storage devices before disconnecting them or powering them off.

Data corruption is often encountered through an external virus stored or installed within the target computer or device. The virus overwrites the original data, modifies the code or permanently deletes it. Besides viruses, data corruption may also occur as a result of hardware or software malfunctions, errors and extreme climate changes. Data can be restored through a backup copy or it can be rebuilt using various data integrity checking algorithms.

Measures to prevent data corruption include:

1. Periodic backup and recovery process.

2. Perform the small amount of regular maintenance.


4. Properly Eject external storage devices and drives, before either disconnecting them or turning them off.
3.3.4 Spyware:
Federal Trade Commission defines spyware as software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer’s consent, or asserts control over a computer without the consumer’s knowledge.\(^{17}\)

Spyware monitors user activity on the Internet and transmits that information in the background to someone else. It heavily consumes computer's memory resources and also steals bandwidth for sending information back to the spyware's home base via the user's Internet connection.

Spy software can record your keystrokes as you type them, passwords, credit card numbers, sensitive information, where you surf, chat logs, and can even take random screenshots of your activity. Basically whatever you do on the computer is completely viewable by the spy. You do not have to be connected to the Internet to be spied upon.

Spyware is often sold as a spouse monitor, child monitor, a surveillance tool or simply as a tool to spy on users to gain unauthorized access. Also known as snoopware, PC surveillance, key logger, system recorders, Parental control software, PC recorder, Detective software and Internet monitoring software.\(^{18}\)

Some commercial firms have released products dedicated to remove or block spyware. Programs such as PC Tools' Spyware Doctor, Lavasoft's Ad-Aware SE and Patrick Kolla's Spybot - Search & Destroy gained popularity as tools to remove, and in some cases block spyware programs.
Many Internet users were introduced to spyware in 1999, when a popular freeware game called "Elf Bowling" came bundled with tracking software. Software designed to serve advertising, known as adware, can usually be thought of as spyware as well because it almost invariably includes components for tracking and reporting user information. However, marketing firms object to having their products called ‘spyware’. As a result, McAfee (the Internet security company) and others now refer to such applications as “potentially unwanted programs” (PUP).

3.3.5 Denial-of-service (DoS):
Network working group of IAB in its RFC 4732 has defined DoS as “an attack in which one or more machines target a victim and attempt to prevent the victim from doing useful work. The victim can be a network server, client or router, a network link or an entire network, an individual Internet user or a company doing business using the Internet, an Internet Service Provider (ISP), country, or any combination of or variant on these”.

In a normal DoS attack, the attacker will overload a site’s server with requests for access far above the capacity of the site, meaning that authentic requests cannot be processed, or saturating the target machine with external communications requests, so much so that it cannot respond to original traffic and responds so slowly so as to be treated as unavailable. In other words DoS attacks are executed by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended services. DoS an also obstruct the communication media between the intended users and the victim so that they can no longer communicate effectively.
The five basic methods of executing the DoS attack are:

1. Over usage of computational resources, such as bandwidth, disk space, or processor time.
2. Destruction of configuration information, such as routing information.
3. Disturbance of state information, such as voluntary resetting of TCP sessions.
4. Disruption of physical network components.
5. Creating hindrance between media and the intended users so that they can no longer communicate properly.

Some of the names associated with DoS attacks are here:
The DDoS names range from mildly amusing to disturbing

1. Ping of Death - create huge electronic packets and sends them on to victims.
2. Mailbomb - send a massive amount of e-mail, crashing e-mail servers.
4. Teardrop - send pieces of illegal packet; the victim system tries to recombine the pieces into a packet and crashes as a result

Protective methods to prevent DoS attacks include: maintaining a firewall, utilizing router filters, disabling unused networks, having a switch with automatic monitoring for DoS attacks.

Changwang Zhang and his research team had proposed an algorithm called as Robust RED (RRED) algorithm to prevent against LDoS attacks. The
basic idea behind the RRED is to detect and filter out attack packets before a normal RED algorithm is applied to incoming flows. They have conducted a set of simulations to evaluate the performance of the proposed RRED algorithm. The results show that, the RRED algorithm nearly fully preserves the TCP throughput in the presence of LDoS attacks.\textsuperscript{20}

3.3.6 Illegal Access:
Anyone who copies, uses or obtains access to computer data from a computer system without permission, where such is required, is termed as illegal access. The offence is often committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

When committed intentionally, the access to the whole or any part of computer system without right then it is considered as criminal offence and shall be eligible for legislative appeal.

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 and mobile phones (SMS/MMS) are categorised as cyber crimes.\textsuperscript{21}

3.3.7 Identity Theft:
It is a kind of cyber crime or fraud in which an individual or a group looses personal data, such as passwords, user names, banking information, or credit card numbers. Online identity theft is sometimes also known as phishing. This is an old practice by cyber criminals or hackers to find ways
to illegally acquire people's personal information through confidence scams (also known as social engineering), stealing mail from mailboxes, or even looking through trash cans or dumpsters. Now that identity theft has moved online, criminals can scam greater numbers of people, which makes it much more profitable.

An individual’s identity may be stolen in the following ways.

1. Attacking computers that don't have firewalls installed.
2. Installing keystroke loggers or other malicious code by hiding it in email attachments.
3. Exploiting browser loopholes that have not been properly patched.
4. Cracking weak or poorly protected passwords.
5. Hiding malicious code in downloads or free softwares.
6. Hiding malicious code in images on websites and waiting for Un-suspecting users to click on them.
7. Spoiling poorly installed networks, and especially wireless home networks.

3.3.7.1 Safe methods to avoid identity theft:

1. Make sure all computers you use in your home or business have the latest firewalls and anti-virus software installed.
2. Keep up-to-date with the latest patches, especially for your browser.
3. Use a good-quality anti-spyware solution, and scan your computers regularly for any pests.
4. Be careful about the types of websites you visit, what you click on, and what you download.
5. Scrutinize suspicious emails that may actually be phishing scams.
3.4 **Executor may include:**
People or a group having potential knowledge and practice of causing soft damage, for some commercial gain are the real executors. Executor are often specialised and hired for committing a cybercrime, sometime very serious and on some occasions just to inform a loophole in the system.

3.4.1 **Hackers (Eavesdroppers)**
A person having a sound technical knowledge in seeking and exploiting the weaknesses in the computer system or computer network compromising computer security is often termed as hacker. This act is motivated by several reasons such as profit, protest or challenge. A team of computer programmers has argued that a person having such skills of breaking into computers may me referred to as a cracker. Clifford R.D. proposes the act of cracking is to “gain unauthorized access to a computer in order to commit another crime such as destroying information contained in that system. Although, arguably, hacking is a criminal offence, we do not include hack-tivists into our definition of “organised criminals.” Organised criminals are only motivated by profit, and they perpetrate the most complicated, costly and critical attacks”.  
The literal meaning the term hacking and the activities of a hacker is a matter of long term controversy. The term hacker is reclaimed by computer programmers who argue that someone breaking into computers is better called a cracker, not making a difference between computer criminals (black hats) and computer security experts (white hats). Some white hat hackers claim that they also deserve the title hacker, and that only black hats should be called crackers.
A person who enjoys exploring the details of programmable systems and stretching their capabilities, as opposed to most users, who prefer to learn only the minimum necessary, this quoted by Jargon file. The Internet Users Glossary simplifies this meaning as “A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular”. 24

Subgroups of the computer hacking world differentiates themselves on the basis of type and reason for hacking and try to leave some groups where they do not agree. Some types are mentioned here. 25,26,27,28

White hat: Breaks security for non-destructive reasons, sometimes to test their own security system while working for a software security company. The term "white hat" refers to an ethical hacker. Also includes individuals who perform penetration tests and openness assessments within a contractual agreement. The EC-Council, also known as the International Council of Electronic Commerce Consultants, is one of those organizations that have developed certifications, course-ware, classes, and online training covering ethical Hacking.

1. Black hat: Violates computer security for personal gain Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network.

2. Grey hat: It is a combination of a black hat and a white hat hacker. A grey hat hacker may surf the internet and hack into a computer system for the purpose of notifying the administrator that their system has a security fault, for example. Then they may offer to correct the defect for a fee.
3. **Elite hacker:** Used to describe the most skilled and often considered a social status among hackers. Newly discovered exploits will circulate among these hackers.

4. **Script kiddie:** Is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept hence the term script.

5. **Neophyte:** Is someone who is new to hacking and has almost no knowledge or experience of the workings of technology, and hacking.

6. **Blue hat:** A blue hat hacker is used to bug test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term Blue-Hat to represent a series of security briefing events.

7. **Hacktivist:** Utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

8. **Nation state:** Intelligence agencies and cyber-warfare operatives of nation states.

9. **Organized criminal gangs:** Groups of hackers that carry out organized criminal activities for profit.

10. **Bots:** These are some software tools which are automated and sometimes free to be used by hackers in carrying out the intended hacking activity.
3.4.2 Cyber-criminals:
People or group of people notoriously involved in harmful exploitation of information and communication technologies are known as Cyber-criminals. Using there harmful skills they steal people's identities, hack into their accounts, trick them into revealing the information, or infect their devices with malware. These professional criminals treat cyber crime like a business and have formed global criminal communities. Combining and sharing methods and tools they even have the capability to launch a coordinated attack. Stolen information and identities can be sold at underground marketplaces which have been formed with mutual understanding.

Taking advantage of global internet connectivity criminals often do things anonymously from any part of the world and sometimes cracking them down becomes very difficult. Cyber attacks are usually done from a far distance by taking control of the intended infrastructure. Difference in cyber laws among countries makes it really complicated to track down these criminals.

One of the prominent tools used by a cyber-criminal is social engineering which is an approach that uses lies to trick people into revealing their personal information. Social engineering attacks frequently involve very convincing fake stories to attract victims into their trap. Kevin Mitnick is one of the most famous social engineers in the world who popularized the term “social engineering.” He explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system.
Chris Hadnagy defines Neuro-Linguistic Hacking (NLH) as a combination and use of key parts of neuro-linguistic programming, the functionality of micro-expressions, body language, gestures and blend it all together to understand how to “hack” the human infrastructure. NLP is how to use the language of the mind to consistently achieve, modify and alter our specific and desired outcomes (or that of a target).29

Common social engineering attacks include:

a. An email that claims there's a problem with victims account and has a link to a fake website. If we put account information into the site it sends that information straight to the cyber criminal (phishing)

b. Request victims to open email attachments that contain malware by claiming it is something they might enjoy (like a game) or need (like anti-malware software)

c. Identify itself to be a network or account administrator and asking for the victim's password to perform maintenance.

d. Announcing that the victim has won a prize but must give their credit card information in order to receive it.

e. Tactfully gather victim’s password for an Internet service and then using the same password to access other accounts and services since many people re-use the same password.

f. Give false promises that the victim will receive millions of dollars, if they will help out the sender by giving them money or their bank account information.
3.4.3 Cyber-warriors:
A person engaged in cyber war, using information technology for personal reasons or due to patriotic feelings or religious belief is usually called as Cyber-warriors. This Cyber war may be initiated either to defend computer and information systems, or to attack them. They are categorised depending on their roles, but all deal with information security in one form or another.

They may attack computers or information systems through hacking or other related strategies, or defend them from their enemies. Cyber-warriors also may find better ways to secure a system by finding shortcomings through hacking and other means, and closing those shortcomings before other hackers find and take advantage of them. Cory Janssen co-founder of Janalta Interactive Inc, the parent company of techopedia tries to explain Cyber-warrior taking example of United States.30

“Countries that are unable to match the U.S. in terms of military technology have resorted to cyber warfare, a method that can still do a lot of damage in terms of economic cost. Various agencies in the U.S. are under constant attack from numerous countries. In response, the U.S. military is training war veterans and wounded soldiers who can no longer fight in the field in the art of cyber warfare to become cyber warriors and continue defending their country in this new form of battle. Given this, the term cyber-warrior has different meanings depending on context in which it is used; the term may refer to someone with malicious intent (the attacker) or a professional who is working to defend against such attackers. The latter context is an emerging career field, similar to ethical hacking”. 
References:

S. Raymond, “Jargon File: Cracker”, by hackers in defence against journalistic misuse of hacker 1985


Blue hat hacker Definition, ‘PC Magazine Encyclopedia’, “A security professional invited by Microsoft to find vulnerabilities in Windows”

