A Brief review on Cyber Crime - Growth and Evolution

Jitender K Malik*, Dr. Sanjaya Choudhury

**Research Associate, Department of Law, Bhagwant University, Ajmer (Raj.) –India*

Abstract:

Since the act of deleting data using a physical device to copy malicious code has not been committed through global electronic networks, it would not qualify as cybercrime under the narrow definition above. Such acts would only qualify as cybercrime under a definition based on a broader description, including acts such as illegal data interference. With the advent and growth of electronic communication, the word "cyberspace" has entered into everyday parlance. In common parlance, 'cyberspace' is the environment in which communication over computer networks occurs. Almost everybody in one way or the other is connected to it: Ladies in the market are connected to it to run their businesses; shepherds are connected to locate their cattle; hunters are connected to it to locate their prey; and our friends in the remote areas are also connected to it. The word "cyberspace" has invaded our collective consciousness like no other. As the technology improves and ownership of home computers increases, one competently navigate his way around cyberspace, downloading information, reading and writing to newsgroups, and receiving and sending emails. Cyberspace represents the new medium of communication, electronic communication, which is fast outmoding, or even replacing, more traditional methods of communication. The present Study attempts a comprehensive definition of the term 'cyberspace,' traces out the evolution and growth of cyber space; and enumerates the pros and cons of information technology.

Key Words: *cyberspace, cyber-attacks, communication.*

1. Introduction:

The variety of approaches, as well as the related problems, demonstrates that there are considerable difficulties in defining the terms "computer crime" and "cybercrime." The term "cybercrime" is used to describe a range of offences including traditional computer crimes, as well as network crimes. As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the different regional and international legal approaches to address the issue, whilst excluding traditional crimes that are just facilitated by using hardware. The fact that there is no single definition of "cybercrime" need not be important, as long as the term is not used as a legal term. The term "cyber" has been used to describe

almost anything that is connected with networks and computers. Unfortunately, however, there is no consensus on what "cyberspace" is. In order to clarify this situation, Ottis, R. & Lorents offer the following definition: "cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems."[1] They describe the background of the definition and show why this approach may be preferable over others. Specifically, they revisit the terms coined by Norbert Wiener (the father of cybernetics) and William Gibson. The authors show that time-dependence is an overlooked aspect of cyber space and make a case for including it in their proposed definition. In addition, they look at the implications that can be drawn from the time-dependence of cyberspace, especially in regard to cyber conflicts, which they define as a confrontation between two or more parties, where at least one party uses cyber-attacks against the other(s). Specifically the authors review the implications on the potential for rapid deployments of offensive and defensive actions in cyberspace, the feasibility of mapping cyberspace, and the need for constant patrolling and reconnaissance.

William Gibson, who used the word for the first time remarked: "Cyberspace: a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts … A graphic representation of data abstracted from the banks of every computer in the human system."[2] These words, written by the science fiction writer, introduced the concept of cyberspace into the English language. But what does cyberspace mean today? There are in fact two spurs of cyberspace. On the one hand, we have virtual reality—a 3-D cyber-spatial environment which humans can 'enter' and 'move through', interacting with both the computer and other human beings, as depicted in films like The Lawnmower Man and Disclosure. On the other hand, we have the slightly less dramatic, but more utilitarian, world of networks of computers linked via cables and routers (similar to telephone connections) which enable us to communicate, store and retrieve information. By far the largest and most well-known of these is the Internet— originally used for email, ftp (file transfer), bulletin boards and newsgroups, and telnet (remote computer access), and now even more of a household name courtesy of the World Wide Web, which allows simple stress-free navigation of the network. This second spur of cyberspace encompasses not only the connections between computers, but also the browser and email software which transmits information, *plus* the internal space of the microchip and other electronic storage technologies—the places in which information actually resides.[3]

The International Telecommunication Union (ITU) states the terms cyberspace, cyber environment and critical information infrastructure are used interchangeably.[4] The definition of cyber world is close to the definition of the cyber environment in ITU-T, which says that the cyber environment 'includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks.'[5] Hathaway and Klimburg present similar thinking when they argue that cyber space contains people and social interaction in the networks in addition to hardware, software and information systems of the internet.[6] The cyber world includes not only the computers and data and information networks, but also the complete and comprehensive system of human existence in those networks. This interpretation of the concept of cyber world allows pondering the essential issues and phenomena that emerge

from this novel domain. These issues include human social behaviour supported by information technical solutions.[7]

The Oxford English Dictionary defines "cyber space" as the space of virtual reality; the notional environment within which electronic communication (esp. *via* the Internet) occurs.[8] According to the UK Cyber Security Strategy, 2011, cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services. In US context, cyberspace is defined as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.[9]

In New Zealand literature, cyber space denotes the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place.[10] To the Germans, cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.[11] Canada's Cyber Security Strategy defines cyberspace as the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship.[12]

Although several definitions of cyberspace can be found both in scientific literature and in official governmental sources, there is no fully agreed official definition yet. According to F. D. Kramer there are 28 different definitions of the term cyberspace.[13]The most recent draft definition is the following: Cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources.

Cyberspace includes:

(i) Physical infrastructures and telecommunications devices that allow for the connection of technological and communication system networks, understood in the broadest sense (SCADA devices, smart phones/tablets, computers, servers, etc.);

(ii) Computer systems and the related software that guarantee the domain's basic operational functioning and connectivity;

(iii) Networks between computer systems;

(iv) Networks of networks that connect computer systems (the distinction between networks and networks of networks is mainly organizational);

(v) The access nodes of users and intermediaries routing nodes;

(vi) Constituent data (or resident data).

Often, in common parlance, networks of networks are called Internet (with a lowercase 'i'), while networks between computers are called intranet. Internet (with a capital 'I', in journalistic language sometimes called the Net) can be considered a part of the system a). A distinctive and constitutive feature of cyberspace is that no central entity exercises control over all the networks that make up this new domain. [14] Just as in the real world there is no world government, cyberspace lacks an institutionally predefined hierarchical centre. To cyberspace, a domain without a hierarchical ordering principle, we can therefore extend the definition of international politics coined by Kenneth Waltz: as being "with no system of law enforceable." This does not mean that the dimension of power in cyberspace is absent; the power is dispersed and scattered into a thousand invisible streams; and that it is evenly spread across myriad people and organizations, as some scholars had predicted. On the contrary, cyberspace is characterized by a precise structuring of hierarchies of power. The Joint Chiefs of Staff of the United States Department of Defense define cyberspace as one of five interdependent domains, the remaining four being land, air, maritime, and space.[15]

Without questioning the validity of the definitions of cyberspace, one can make the following observations:

- Virtually all definitions agree that cyberspace includes tangible elements. This would imply that cyberspace cannot exist without tangible elements.
- Virtually all definitions agree that cyberspace must include information. Information can either be stored data, signalling between processes and/or devices or as a content that is being transmitted.
- Cyberspace includes tangibles but, at the same time, it is also virtual.
- Only a few definitions consider activities and interactions (within cyberspace) part of cyberspace.
- Probably contrary to popular beliefs, networks and Internet are not necessarily part nor are required for cyberspace but they are still 'desired.' Interconnectedness seems to have an equal weight as the Internet itself.

In conclusion one can say that different organizations have adopted different definitions of what cyberspace means. Some of them – like the EU – do not have an official definition at all, but that does not prevent it from discussing the term. The parent term of cyberspace is "cybernetics," derived from the ancient Greek- *kybernētēs* - which means steersman, governor, pilot, or rudder, a word introduced by Norbert Wiener for his pioneering

work in electronic communication and control science. This word cyberspace first appeared in the art installation of the same name by Danish artist Susanne Ussing.[16]

2. Evolution and growth of cyber space

The construction of cyberspace is creating new challenges for the social sciences, the full nature of which still remains to be fully understood - perhaps even calling into question some of its most basic assumptions.[17] Although it may seem like a new idea, the net has actually been around for over four decades. It all began in the United States during the Cold War, as a university experiment in military communications. The decision was made to link lots of computers together in a network instead of serially (in a straight line). The Pentagon thought that if there was a nuclear attack on the United States, it was unlikely that the entire network would be damaged, and therefore they would still be able to send and receive intelligence.

At first each computer was physically linked by cable to the next computer, but this method had obvious limitations. The problem was corrected by the development of networks utilizing the telephone system. Predictably, people found that nuclear strike or not, they could talk to each other using this computer network. Eventually, some university students started using this network to do their homework together.

It seems a natural human characteristic to want to communicate, and once people realized that they could talk to other people using this computer network they began to demand access. At first, the users were only from the university and government sectors. But more and more people could see the possibilities of computer networks, and various community groups developed networks separate from the official networks to be used in their local communities.

Add all of these various local, regional and national networks together and we have the Internet as we experience it today - an ever expanding network of people, computers and information. Today the Internet is being used in ways the Pentagon never dreamed of four decades ago. What began as an exercise in military paranoia or suspicion has become a method of global communication.

"Cyberspace" is a term coined by William Gibson in his fantasy novel *Neuromancer* to describe the "world" of computers, and the society that gathers around them.[18] Gibson's fantasy of a world of connected computers has moved into a present reality in the form of the Internet. In cyberspace people "exist" in the ether- you meet them electronically, in a disembodied, faceless form.

The rapidly shifting terrain of cyberspace includes not only the Internet, but also the legacy telephony infrastructure, cellular phone technologies, and wireless data services. The technologies underlying all of these aspects of cyberspace—such as bandwidth, interconnectedness, processor speed, functionality, and security vulnerabilities— have evolved over decades.

3 The three major trends

The purpose of this section is to identify these evolutionary trends and to extrapolate their implications. This section focuses on the accumulation of incremental evolutionary change over long periods. Even individually small quantitative changes, when compounded over time, can bring about great qualitative changes on their own. In addition to evolutionary trends, revolutions are also possible. Trends that have transformative implications will be examined, while fads and "flash-in-the-pan" issues will be ignored, even though it is not always easy to see the difference while in the midst of major transformations.[19]

Trends that have transformative implications shall be categorized into three types:

(i) Computer and network trend;
(ii) Software trend; and
(iii) Social trend.

Computer and network trends include: increases in computer and network power; proliferation of broadband connectivity; proliferation of wireless connectivity; transition from Internet Protocol version 4 (IPv4) to IPv6. Software trends include: increases in software complexity; enhanced capabilities for search both across local systems and Internet-wide; widespread virtualization of operating systems convergence of technologies; increased noise in most aspects of cyberspace; increased vulnerability due to advancement of computer and network attack and exploit methodologies. Social trends in the use and development of cyberspace include: worldwide technological development with different local emphases; rise in online communities, collaboration, and information-sharing.

Cyberspace evolution is proceeding on a multitude of fronts. These trends point to a future in which cyberspace becomes far more pervasive; touching most aspects of daily life in some way for a majority of the world. Two longstanding trends—significantly lower cost of processor performance and increases in flexible network connectivity—will facilitate the incorporation of cyberspace into more and more products. If these trends continue, some form of intelligence and network communication will eventually be embedded in most electrically powered devices. These trends mean that cyberspace is increasingly becoming an overlay technical infrastructure to the physical world, as it increasingly becomes involved in monitoring, analyzing, and altering the physical landscape.

3.1.1 Computer and network trends

Among the computer and network trends likely to have lasting effect are: increases in computer and network power, proliferation of broadband and wireless connectivity, and upgrades in the fundamental protocols of the Internet.

- **Increase in computer and network power**

Moore's law describes a major component of the evolution of the information technology industry. Originally observed in 1965 by Gordon Moore, co-founder of Intel Corporation, Moore's law posits that industry's ability to produce integrated circuits continually improves, so that the number of micro components that can be etched on a chip will double at regular intervals.[20] There is some variation in the specific interval cited for the doubling timeframe observed by the law. Gordon Moore originally predicted doubling each year but later revised the timeframe to two years. Historically, the timeframe has varied between one and two years. Most current estimates focus on the two-year timeframe. The doubling in the density of circuitry translates to increased processor performance and lower costs. Although the slowdown and even ultimate demise of Moore's law are predicted from time to time, the pace it describes has continued for over four decades. It should be noted that, although Moore's observation is commonly referred to as "Moore's law," it is an observation and an industry goal, not a "law" in the physical sense.

As individual machines grow more powerful, they are also increasingly interconnected in networks. The benefits of the increase in interconnectivity are addressed in Metcalfe's law, named after Robert Metcalfe, one of the inventors of Ethernet technology. Metcalfe posited that the value of a telecommunications network is proportional to the square of the number of its users. According to this hypothesis, as more users are brought onto a shared communications network, the value of the network to the overall community grows not just at a linear rate, but as the square of the number of users. A related hypothesis, Reed's law, estimates the value even higher, saying that the utility of a network can scale exponentially with the number of participants in the network. [21]

Unlike Moore's law, which has demonstrably reflected reality for the past four or more decades, Metcalfe's and Reed's laws cannot be quantified: they are more a metaphorical statement of the value and power of networks than a quantifiable observation or prediction. Furthermore, Metcalfe's and Reed's laws have been challenged; some observers have said that they overstate the increase in value of a network when new users join. Still, it is generally agreed that the value of a network grows faster than at a linear rate of the number of users. Well established technological and economic trends led to the observations known as Moore's law and Metcalfe's law; these trends suggest that the future of cyberspace will see faster computing devices interconnected in more powerful and valuable networks. With the compounding impact of these trends over time, cyberspace will continue to grow in importance and influence as more economic, military, and even social activity migrates to that realm.

- **Broadband proliferation**

Another major evolutionary trend in cyberspace is the widespread deployment of broadband Internet services. Cyberspace experienced at a speed of just 56 kilobytes per second, allowing rudimentary Web surfing and data exchange—is very different from

cyberspace at 400 kbps or more. Widespread access to faster connectivity by desktops, laptops, personal digital assistants, and cell phones enables new business models and new social interactions. Just as business and social models were transformed by the move from trains and ocean liners to jet airline flights in the past century, today the richer audio, video, and networked applications supported by higher speed Internet connections make cyberspace significantly more valuable to its users. Many face-to-face transactions and physical exchanges can be supplanted by much less expensive software-based interactions. New services not previously associated with the Internet, including telephony and television, are moving to this plentiful cheap bandwidth. Widespread fiber optics, cable modems, digital subscriber loops/lines (DSL), and broadband wireless services are the technological underpinnings allowing broadband access by consumers or businesses throughout the world.[22]

These technologies have higher speeds (typically greater than 400 kbps) and are also always on, not requiring time-consuming dial-up "handshakes." While broadband deployment is already a reality in many parts of the world, it is not yet universal. Some set of users probably will continue to use dial-up access for some time, but there are likely to be fewer and fewer. Broadband connectivity to the endpoints of computer communication is only possible if the Internet backbone itself can carry all of the extra traffic generated by these end systems. Internet backbone providers have deployed more high-speed links, using new fiber technologies such as OC–48 and OC– 192 with operating speeds of 2.488 Gigabits per second and 10 Gigabits per second, respectively.[23]

Higher speed satellite and microwave towers are interconnecting high-speed networks around the world. Interconnectivity between various backbone providers has increased to carry more traffic more quickly. As this interconnectivity grows, the topology of the Internet backbone becomes more complex from a design and management perspective. As client computers increasingly rely on broadband access, and as the Internet infrastructure is refined to carry all of those bits, the servers to which the communications are directed likewise need additional computational and network power to provide new services. Faster servers can help deal with some of these needs, but most large Internet companies are instead relying on larger numbers of less expensive servers, distributed across one or more campuses around the world. Large Internet companies[24] are constructing vast "server farms." For instance, Google's server count was half a million computers in 2007.

Business models are also evolving, as Internet service providers (ISPs) try to furnish value-added services and applications on top of their increasingly commoditized bandwidth business. To realize the business value in the telephony, video, and various other applications and content being distributed via their "pipes," some ISPs are partnering with, buying, or building in-house application services and content. Such services and content are directly affiliated with that ISP, in contrast to other services that are not affiliated but that are accessed through that ISP by its customers. This evolution has led some ISPs to consider charging non-affiliated application service providers and users a premium for their use of

high bandwidth. Those that do not pay extra may face lower performance, with their traffic handled at a lower priority than higher paying affiliated users and application providers.

This economic friction between ISPs and application service providers is a worldwide phenomenon and has been termed the "Net neutrality" issue. Some argue that governments should require the equal or "neutral" handling of affiliate and non-affiliate traffic alike by ISPs, to foster interoperability and prevent the fragmentation of the Internet into various ISP enclaves. Others argue that allowing economic advantages for an ISP's affiliated services will encourage investment in new and improved services by the ISPs. Several countries are grappling with this complex and contentious issue.[25] In the future, bandwidth to the end system and on the backbone will likely grow even faster, with more widespread deployment of 10 megabits per second or higher rates to the home and a corresponding backbone to support it. Video applications will almost certainly increase, as today's nascent Internet television business grows much larger and video conferencing is more widely used.

- **Wireless proliferation**

Cyberspace connectivity is increasingly moving to wireless communication, in the form of wireless local area networks (WLANs), wireless broadband, and similar technologies. One of the major vectors of this move is often overlooked in discussions of cyberspace: the cell phone. An estimated two billion people have access to cell phones. Over 150 million camera phones have been sold to date, each supporting voice, text, and image transfer. Even with low bandwidth text messaging, their small size, decentralized communications capacity and relatively low cost have made cell phones an increasingly important technology underlying social change.[26]

Where today's cell phones have simple text messaging and still cameras, future cell phones with higher bandwidth applications and full video capabilities are likely to have even greater impact as they gain the capabilities of modern personal computers and become, in effect, pocket-sized television studios. The hand-held video cameras of the late 1980s and early 1990s led to countless major news stories, such as the 1992 Rodney King riots in Los Angeles. However, that technology was limited: few people carried cameras with them most of the time, and the technology required the cumbersome handling of physical videotapes, typically delivered by hand or by courier.

By contrast, when a major portion of the world's population carries cell phone–based video cameras wirelessly linked to the Internet at all times, cell phones will likely have a much larger impact on society, as when camera-equipped cell phones disseminated graphic pictures and video, *albeit* of low quality, of the execution of Saddam Hussein in 2006 within minutes of the event. Today's grainy cell phone photos and simple videos will be replaced by much better multi-megapixel video cameras integrated into cell phones as video capture technology becomes smaller, cheaper, and more widely disseminated. Already television news outlets in some countries ask members of the public to submit cell phone video of events immediately after they happen. Web sites offer to broker the sale of videos of hot

news events taken by private individuals. These trends decrease the time between an event's occurrence and its coverage in the news, further shrinking the news reporting cycle and the time available for the public and policymakers to analyze events.

Numerous other wireless technologies are transforming the nature of cyberspace. WLANs, in their most popular form, are implemented according to a set of standards denominated "802.11." Such "Wi-Fi" networks allow nearby systems (within perhaps 100 meters) communicating with one another or gaining access to the Internet. Computers from wired access make it possible to use them for a wider variety of applications, ranging from industrial use to home appliances. By minimizing the need for costly wiring installations, WLANs allow for more rapid network deployment at much lower costs. A variety of organizations have taken advantage of this.[27]

WLAN technology is pushing the boundaries of the definition of "local" as well: originally designed for shorter distances, 802.11 signals have been successfully carried several miles and have been detected at over 200 miles under ideal circumstances (atop mountains on a clear day). Wireless signal transmission for computer devices often outpaces the distances it was designed to span. While WLAN technologies were created for distances up to 100 meters, their propagation across a mile or more has significant implications. Most consumers would be surprised to hear that the WLANs they have deployed in their homes can be detected and even accessed many blocks or miles away. Wireless data communications opens up computer network access over longer distances, making computers more accessible to both their users and would-be attackers. With widespread deployment of WLANs, numerous wireless networks often occupy overlapping physical spaces.

Activating a wireless detection device in any major city typically reveals at least half-dozen nearby WLANs ready for a connection. Systems may appear on a WLAN for a short time, use it to transmit some vital information, and quickly disappear; this makes it hard to determine which assets are part of a given organization's network and which are not. For enterprises, maintaining a list of computing assets in such environments is difficult. And if an enterprise does not know which machines are part of its network and which are not, managing and securing those assets becomes impossible. Another rapidly rising wireless technology is evolution data optimized (EVDO) service, by which cellular networks make possible high-speed data transmission from PCs and cell phones. EVDO is an evolutionary descendant of code division multiple access (CDMA) technology used by some cell phones for wireless data transmission.

In the United States, a handful of carriers have deployed networks that use EVDO and CDMA technology, allowing business users and consumers in most major cities wireless connectivity at 128 kbps to two Mbps over distances of a mile or more. With a simple PC card, cell phone and PC users can gain wireless broadband access to the Internet from most major population centres in the United States. Such services could supplant cable modems and DSL, allowing more mobility at high bandwidths over longer distances. Another emerging wireless technology is Worldwide Interoperability for Microwave Access

(WiMAX), designed to obviate expensive copper and fibre solutions for the "last mile" to consumers' homes.[28]

WiMAX deployment is beginning to be used in urban and suburban areas to link Wi-Fi LANs and to connect users to their ISPs. Other wireless technologies, such as Bluetooth, are interconnecting the components of an individual computer wirelessly over distances of up to 10 meters. Bluetooth capabilities are built into many modern laptops, keyboards, computer mouse devices, cell phones, headsets, and music players. While designed for distances of only 10 meters, hobbyists have discovered that Bluetooth signals can sometimes be detected over a mile away. With numerous Bluetooth enabled devices in close proximity, it can be hard to determine which assets form part of a given computer and which belong to another, again complicating the management and security of assets that are increasingly ephemerally tied to the network via wireless.

Another rapidly rising wireless technology is Radio Frequency Identifier (RFID) tags very small, simple computer chips that send a unique identifier number. They are being used to support inventory activities, augmenting and possibly someday supplanting the familiar Universal Product Code barcodes found on nearly all products today. With RFID tags, which are about the size of a grain of rice, a given product's code can be read without line-of-site viewing or direct physical access, as long as the radio frequency transmission can be read. RFIDs were designed to communicate over short distances (originally one to ten meters, but hobbyists have demonstrated reading such tags over 100 meters away). Codes identifying equipment can be read without physical contact over such distances; with possible privacy implications as RFID applications spread.[29]

As RFID deployment becomes more prominent, implementation vulnerabilities are likely to be discovered and scrutinized. Researchers have begun to devise methods for attacking RFID infrastructures, devising hypothetical worms that could spread from tag to tag, and infecting large numbers of systems with very simple code. Research on attacks against RFID readers, including the transmission of malicious code to such readers, is also under way. RFID spoofing, whereby an attacker makes a bogus RFID tag impersonate another legitimate tag, is an active area of research today with implications on cloning passports.

Skimming is the process of surreptitiously reading an RFID tag to extract its vital information, which may later be used in a spoofing attack to clone the tag. With RFID information embedded into consumer products, sensors deployed in a city could instantly determine the products carried by citizens who walk within 100 meters of the sensors, allowing monitors to determine the make and model of various devices carried by the user—an issue with significant privacy implications. Very invasive remote search of pedestrians or houses by government and law enforcement officials (as well as thieves) becomes possible with the technology.

- **Transition from IPv4 to IPv6**

The current Internet infrastructure is based on the widely deployed IPv4, a specification originally created in the late 1970s that spread widely in the early 1980s and throughout the 1990s as the Internet grew. This protocol far exceeded its original expectations, becoming the common language for communication across the Internet and large numbers of private networks, and allowing a huge variety of devices—from mainframe systems to cell phones—to communicate. Despite its unprecedented success as a protocol, the original IPv4 design had significant drawbacks: a limited number of network addresses that were distributed inefficiently, no built-in support for security, a lack of quality-of-service features, and limited support for mobile devices.

To address these shortcomings, the Internet Engineering Task Force set out in the mid-1990s to define a next-generation Internet protocol, termed IPv6. While the IPv6 specifications were completed sometime ago, full deployment has been slow. Most modern operating systems have IPv6 software, but few use it. Pockets of IPv6 networks exist in specialized laboratory and educational environments. Small IPv6 networks have been overlaid on the existing IPv4 Internet, with network nodes run by academics, researchers, and hobbyists around the world. One of the major reasons IPv6 deployment has moved slowly involves the innovative retrofitting of its various concepts into the existing IPv4.[30] Most organizations have deployed various network address translation devices to shuffle and reuse private network addresses, somewhat alleviating the original constraints of IPv4's 32-bit addresses. Likewise, quality-of-service and mobility options have been implemented in IPv4. These adaptations to IPv4's limits have eased many of the "pain points" driving the demand for IPv6.

Although IPv6 deployment has started slowly, it is expected to ramp up; both the Chinese government and the U.S. military have announced intentions to move to IPv6 to support the modernization of their large networks. Even so, some Internet experts have viewed IPv6 deployment as a perpetual "five years in the future"—always predicted, but never actually occurring. However, over the next decade, IPv6 deployment seems very likely, given the momentum of decisions by large buyers, large vendors,[30]and the Internet Engineering Task Force, which crafts the specifications for the protocols used on the Internet.[32]

Building and maintaining IP stacks is very difficult, even using the far simpler IPv4 protocol. The software development community has required a full 20 years to scrub similar problems due to faulty code out of their IPv4 implementations.8 IPv6 software is likely to go through a similar process as vulnerabilities are discovered and fixed. While it may not take another 20 years to get IPv6 right, it will certainly require significant effort to discern flaws in the numerous implementations of this vastly more complex protocol. The Internet and its users may be exposed to attacks for some time. IPv6 also raises other security implications. The very large address space can make it easier for systems to hide: an attacker who

modulates a network address across a very large address space can hide systems more easily than within the smaller and simpler IPv4 landscape.

3.1.2 Software trends

Among the software trends likely to have lasting effect are: increases in software complexity; enhanced capabilities for search both across local systems and Internet-wide; widespread virtualization of operating systems convergence of technologies; increased noise in most aspects of cyberspace; increased vulnerability due to advancement of computer and network attack and exploit methodologies.

- **Increases in software complexity**

Although underlying hardware and network speeds have increased, most new computers do not seem to their users to be significantly faster than their predecessors for very long after their introduction. This is largely due to increases in software complexity, as additional features, increased error-handling capabilities, and more complex security facilities sap the processing gains reflected in Moore's law and in higher bandwidth.[33] Modern software includes a proliferation of features, some important and useful to large numbers of users, and others providing utility to only a small fraction of the user base. Users demand that new programs do more than their old software, and vendors cater to this expectation. Software vendors introduce these features to entice new customers to purchase their products, as well as to inspire existing customers to continue on the treadmill of constant software upgrades. Unfortunately, some software vendors do not spend the resources necessary for thorough development, integration, and testing of these features and modifications.

More complex software is more likely to have flaws, which may manifest themselves in broken features, software crashes, or security vulnerabilities. When a software flaw is discovered, especially one with major security implications, the software vendor typically releases a "patch" to alleviate the condition. Microsoft, for example, releases patches once per month, each typically including between five and a dozen major fixes, often requiring upwards of 10 megabytes of new code. With such massive changes pushed to over 100 million systems, the patching process for Windows alone is a monumental worldwide undertaking on a monthly basis, involving not just Microsoft, but also hundreds of thousands of enterprise users and consumers, not all of whom test such patches carefully before installing.

Moreover, multiple patches applied over time could introduce additional flaws. The constant accumulation of patches can make systems more "brittle," requiring even more complexity to patch adequately without breaking functionality. Unfortunately, complexity is often the enemy of security, as subtle vulnerabilities linger in highly complex, perhaps poorly understood code. To address such vulnerabilities, security tools—antivirus tools, antispyware

software, and intrusion prevention systems—are common defences for systems today. Many of these tools operate in a reactive fashion, to clean up after an infection has occurred, and most defend against specific vulnerabilities that have already been found, not against as-yet-undiscovered security flaws. Compounding the problem, these security tools themselves often have flaws, so they need patches as well. This, again, increases the overall complexity of computer systems and makes them even more brittle. Antivirus, antispyware, and other anti–malicious code technologies use a mixture of techniques to detect such "malware," analyzing protected computers on which they are installed at a granular level to police the system for infection and attacks. The need for such defence is turning into a significant security tax on the increases described by Moore's law and is boosting complexity.

- **Enhanced search capabilities**

With increasingly complex software used for a greater number of applications, more and more vital data is accumulating in databases and file systems. On a local system, data are typically stored in multi-Gigabyte or even Terabyte (1,000 Gigabyte) file systems. On large servers or even networked groups of systems, databases often exceed 100 Terabytes. These data are only useful if users and applications can search for information; high-quality search functionality is therefore vital, and the data must be organized, stored, and presented in useful structures. The metadata that describe the data, tagging, and visualization technologies are thus increasingly critical. Because of their involvement with these crucial functions, Internet search engines are currently at the centre of activity in cyberspace evolution. As search engines acquire more data sources, including phone books, highly detailed satellite imagery, and maps, users are presented with more powerful search directives and operators.[34]

Such options let users hone in on specific items they seek, using a complex array of search directives instead of merely grabbing data with a specific set of search terms located in it. In addition, simple text-based searches are expanding to searches for images, sound, or videos. With so much information on the Internet, many users need help to find what they need. Users might not even know precisely what to search for and would benefit from a ranking system of interesting or useful sources of information. To address this need, other sites on the Internet act as aggregating front-end portals that organize data from multiple data sources and process it to provide users with extra value. Sites such as digg.com and del.icio.us contain lists of popular articles and sites that are voted on by users, giving other users a guide to information in a variety of categories The need for search capabilities is not limited to the Internet. Internal network searching is increasingly important for locating useful information from an organization's internal servers and desktop computers.

To address this need, Google offers an appliance that explores an internal enterprise network and creates a "mini-Google" for that organization, searchable in the same manner as the Internet-wide Google itself. Many other players are also moving into the internal enterprise network search market. Local system search tools are also being deployed, including Google's Desktop Search software, Apple's Spotlight for Macintosh, and Microsoft's enhanced search capabilities for Windows machines. These tools let users

formulate queries to find important information stored on their local hard drives rapidly. Current search capabilities of local products have only a limited syntax of search directives and operators, but these technologies will improve. Search capabilities are particularly vital to analysis of very large centralized data repositories. Services such as LexisNexis (for searches in published news sources and legal documents), credit reporting agencies, and fraud detection tools for financial services organizations require extremely rapid search of large databases maintained by a small number of companies and government agencies. These data sources are used for data mining, correlation, and detailed analysis to discern trends and important outliers. Many of the operators of such databases sell search services to their clients; major economic decisions may be based on the results of searches of these data repositories. System downtime of a credit-reporting database, for example, could have major economic impact. Novel search strategies made Google what it is today; its Page Rank algorithm for associating pages together provides a fast and reliable method for searches. In the future, as data sources and the amount of information stored grow, searching and prioritizing information are likely to become even more important, and new search strategies and new companies will arise to help people use data.

- **Widespread operating system virtualization**

Virtual machine environments (VMEs) such as VMware, Microsoft's Virtual Server, and Xen let a user or administrator run one or more guest operating systems on top of a single host operating system. With such VME tools, for example, three or four instances of the Microsoft Windows operating system can run as guest systems on top of a single Linux host operating system on a single PC or server. The concepts of virtualization were pioneered in the mainframe world but are now migrating to standard PCs and even to cell phone systems. Such virtualized environments are used for clients as well as servers in a variety of commercial, government, and military organizations, and their deployment is increasing very rapidly for several reasons:

(i) VMEs improve server operations by helping to cut hardware costs, simplify maintenance, and improve reliability by consolidating multiple servers onto a single hardware platform.

(ii) They may lower the cost of providing user access to multiple networks having different sensitivity levels. By means of VMEs, some government and military agencies and departments may use one PC, with different guest operating systems associated with each separate network a user may need.

(iii) Numerous "honey pot"[35] defensive technologies rely on VMEs because they can be more easily monitored and reset after a compromise occurs.

(iv) Systems that are directly accessible from the Internet have a high risk of compromise; in multi-tiered e-commerce environments, it can be expected that the front-end system will be compromised. Increasingly, therefore, these exposed hosts are installed on VMEs to minimize downtime, increase security, and simplify forensic procedures.

Computer attackers are, accordingly, becoming very interested in detecting the presence of VMEs, both locally on a potential VME and across the network. If malicious code (such technologies as spyware or keystroke loggers) detects a VME, it might shut off some of its functionality to keep researchers from observing it and devising defences. Researchers might not notice its deeper and more insidious functionality or may have to work harder to determine what the code would do when not in the presence of a VME. Either way, the attacker buys time, and with it, additional profit. VME detection is useful to attackers who seek to avoid wasting time on honey pots.

Attackers also have other motivations for discovering whether a given system is running in a VME. If, for example, an attacker could find out that a group of five systems were guest virtual machines all on a single host, launching a denial-of-service attack against the host machine would be an easier way to cause more harm to the target organization. As VMEs are deployed more widely, even perhaps to a majority of machines on the Internet, their detection may become a less significant issue, as attackers may come to assume they are always in a guest machine. However, other security implications of VMEs would come to the forefront. VME detection could become a precursor to VME escape, whereby an attacker might leak classified information from a more sensitive guest machine to a more easily compromised guest, undermining isolation and exposing sensitive data. An attacker or malicious code that detects a VME might try to move from a guest machine to the host machine or to other guests, compromising security, infecting other guest systems, or breaking into higher levels of security classification.

- **Technological convergence**

Digital convergence, which has been predicted at least since the late 1970s, is starting to happen rapidly.[36] Previously, disparate technologies, such as telephones, radio, television, and desktop computers, increasingly use a common set of underlying technologies and communications networks. Convergence has recently been manifested with the migration of PC based technology—hardware such as processors and hard drives as well as software such as operating systems and browsers—to non-PC products. Internet telephony, for example, is growing rapidly in companies, government agencies, and households, and new phone companies are being formed to provide related services. Many radio stations stream their audio across the Internet to augment their broadcast service and reach new audiences around the world. Music sales on the Internet have been a small share of music sales, but the percentage is increasing rapidly.[37]

Some music playback and video equipment incorporates hard drives to store digitized music files or video footage. Apple, Google, and others now sell or distribute television shows on the Internet, both for streaming[38] and for download.[39] YouTube announced that it handled over 100 million video downloads per day as of mid-2006.[40] These are typically homemade videos or captured broadcast or cable television snippets ranging from two to five minutes in length. Through services such as Google Earth and other satellite and mapping services, cyberspace is influencing perception and use of the physical world. High-quality,

easily available maps allow people to understand their surroundings and even to manipulate them better.

Convergence can help to lower transmission costs for content because a single network—the Internet—can deliver disparate services. Consumers can move content among different types of systems—from a portable music player to a computer to a television, for example. However, from a security and reliability perspective, convergence brings new risks. An attack or an accidental disruption can have a more significant impact because a larger population of users and organizations is relying on a common infrastructure using common technologies. Such disruptions may affect services that users may not realize are related.[41] Major upgrades of converged infrastructure may be more complex because their implications for multiple services must be considered but perhaps cannot all even be anticipated. Most organizations, and the ISPs they rely on, strive not to have potential single points of failure in their physical deployments, but their use of common operating system software [42] may raise the risk of downtime and attack.

As significant services such as telephony, television, and business transactions move to broadband Internet connectivity, modern economies increasingly depend on the Internet infrastructure and on the ISPs. In many countries, competing ISPs have taken on a role filled by monopolistic telephone companies in the past as stewards of the nation's communications infrastructure.[43] In most countries, regulations do not exist for the collection of ISPs and Internet backbone providers, who have nonetheless provided the United States at least with relatively high reliability.

There are even bigger implications as the networks used to manage various critical infrastructures converge with the Internet itself. The supervisory control and data acquisition (SCADA) systems associated with control of electrical power distribution, water distribution, pipelines, and manufacturing are increasingly managed using PC-and Internet-related technologies. Although most SCADA systems are not directly connected to the Internet itself, they are managed via maintenance ports that use the same technologies as the Internet, and even isolated SCADA systems sometimes communicate with laptop PCs that also connect to the Internet from time to time. These maintenance ports could offer a backdoor avenue for attack, exposing SCADA systems.

Once convergence occurs, attacks, infections, and disruptions launched from other aspects of cyberspace could have amplified economic effects. Convergence of technologies also implies convergence of threats and vulnerabilities that thus amplify risk, perhaps in unexpected ways. Even if the SCADA systems themselves could withstand such an attack, the management systems controlling them might be disabled or impaired, affecting control of critical infrastructure facilities and thus preventing alerts and corrective actions in response to an emergency.

Another area of network convergence is the rise of voice over Internet protocol (VoIP) services. The most familiar aspect of VoIP involves end-user telephony; for example, cable companies and others advertise phone service carried over broadband Internet connections.

VoIP, however, is not limited to carrying calls from individuals to their local phone companies: many long- distance companies are already transporting at least some of their long distance traffic by means of IP-based networks to take advantage of the lower costs associated with transporting such calls over broadband pipes that mix Internet data and voice. Even users relying on traditional phone lines—the so-called Plain Old Telephone Service (POTS)—may thus have their calls carried in part over the Internet, unaware that VoIP was associated with the call made POTS- line to POTS-line.

A major concern is that the existing non VoIP long-distance network may not be able to handle all of the long-distance traffic if the Internet and its VoIP systems were impaired. Because design of local and long-distance telephony capacity now presumes that a certain call volume will be handled via VoIP, the telephony infrastructure might not be able to handle the entire load if all VoIP became unavailable due to an Internet attack or outage. This is of particular concern for emergency organizations that must rely on public facilities to communicate, including law enforcement, government, and military groups. The converse could also be a problem, if a cellular outage caused a surge in VoIP calls, overloading the carrying capacity of the Internet. As convergence continues, many more services will be delivered to homes, government agencies, and military operations via combined networks. Even when multiple networks exist, gateways may shuttle information between one network and another, resulting in a network of interconnected networks. The resulting converged systems and networks will offer some highly useful synergies, but at the cost of increased risk

- **Increased noise in most aspects of cyberspace**

As cyberspace has grown, various aspects of it have become full of noise, or apparently random data without meaning to most users or applications. Consider spam, or unsolicited email that typically has a commercial message.[44] Newsgroups often host messages full of apparent nonsense that just takes up space. Another form of cyberspace noise is the clutter of advertisements on major Web sites today, including pop-up ads. Search engine results often include noise, either from mistaken matches returned by search engine software or Web sites that deliberately try to fool search engines in order to be included inappropriately in search results. Uniform resource locators, which point to Web pages, are increasingly cluttered with complex symbols and in some cases even small software snippets designed to run in browsers.

Roving, automated Web crawlers search the Internet looking for Web sites with forms to fill out, which they then populate with advertisements or political messages. The Internet even sees raw packet noise. “Sniffing” software that monitors an unfiltered Internet connection with no regular use will see a significant amount of nonsense traffic, as users around the world inadvertently type incorrect IP addresses, attackers scan for weak target sites, and backscatter is generated by spoofed attacks against other sites. The Internet is indeed a noisy place, and it is growing noisier. Noise is helpful to those wanting to hide: a noisy environment can let covert channels blend in, so attackers can communicate and coordinate.

An attacker might send spam messages, newsgroup postings, or even raw packets to millions of targets on the Internet just to obscure delivery of a single encoded message meant for a single individual or group. Such a message is not likely to be noticed in the day-to-day noise distributed via these same mechanisms. What's more, the location-laundering mechanisms pioneered by the spammers would make it very difficult to find the source of such a message and, given that the message is spewed to millions of destinations, locating the true intended recipient is likewise a major hurdle. Finding an information needle in the haystack of noise data is difficult, and as noise increases, it becomes harder. In the future, the Internet will likely become even noisier, as many new services are deployed that are filled with advertising and nonsensical information. Computer attackers and political dissidents will likely increasingly use this noise to camouflage their plans and communications with each other.

- **Advancement of computer attack and exploitation methodologies**

A major trend fuelling the evolution of computer attacks and exploits involves the rising profit motive associated with malicious code. Some attackers sell to the highest bidder customized malicious code to control victim machines. They may rent out armies of infected systems useful for spam delivery, phishing schemes, denial-of-service attacks, or identity theft. Spyware companies and overly aggressive advertisers buy such code to infiltrate and control victim machines.[45] Organized crime groups may assemble collectives of such attackers to create a business, giving rise to a malicious code industry.

In the late 1990s, most malicious code publicly released was the work of determined hobbyists, but today, attackers have monetized their malicious code; their profit centres throw off funds that can be channelled into research and development to create more powerful malicious software and refined business models, as well as to fund other crimes. When criminals figure out a reliable way to make money from a given kind of crime, incidents of that kind of crime inevitably rise. Computer attackers have devised various business models that are low risk, in that the attackers' chances of being apprehended are very small when they carefully cover their tracks in cyberspace. They can make hundreds of thousands or even many millions of dollars.

A factor fuelling the growth of cyber-attacks is 'bot' software. Named after an abbreviated form of the word robot, this software allows an attacker to control a system across the Internet. A single attacker or group may set up vast botnets— groups of infected machines—scattered around the world. Bot-controlled machines give attackers, economies of scale in launching attacks and allow them to set up virtual super computers that could rival the computer power of a nation- state. They can use that resource to conduct a massive flood, to crack crypto keys or passwords, or to mine for sensitive financial data used in identity theft. Bots and other computer attack tools have become highly modular, using interchangeable software components that allow attackers to alter functionality quickly to launch new kinds of attacks. Common bots today include 50 to 100 different functional

modules; an attacker could shut off or remove those modules not needed for a given attack, while more easily integrating new code features. Other modular attack tools include exploitation frameworks, which create packaged exploitation code that can infiltrate a target machine that is vulnerable.

Just as interchangeable parts revolutionized military equipment in the early 19th century and consumer manufacturing in the early 20th century, interchangeable software components today offer computer attackers and exploiters significant advantages in flexibility and speed of evolution. Speeding up evolution further, attackers increasingly rely on exploit and bot code that morphs itself, dynamically creating a functionally equivalent version with different sets of underlying code. Such polymorphic code helps attackers evade the signature-based detection tools used by the dominant antivirus and antispyware technology of today. This dynamically self-altering code is also harder to filter, given that it constantly modulates its underlying software. This "moving target" of code also makes analysis by defenders more difficult.

Polymorphic code furthers attackers' goals because the longer the attackers have control of a botnet by evading filters and signature-based detection, the more money they can realize from the infected systems. Another trend in attacks involves "phishing" email: an attacker pretending to be a trusted organization or individual sends email that aims to dupe a user into revealing sensitive information or installing malicious software. Attackers often spoof or mimic email from legitimate e-commerce and financial services companies to try to trick a user into surfing to a bogus Web site that appears to be a retailer or bank. When the unsuspecting user enters account information, the attacker harvests this data, using it for identity theft.

More recent phishing attacks include so-called spear phishing attacks that target a particular organization or even individuals. Such phishing email may appear to come from a trusted individual, such as a corporate executive, government manager, or military officer, and exhorts the recipient to take some action. Simply clicking on a link in a spear-phishing email could allow the attacker to exploit the victim's browser, installing a bot on that machine that would act as the attacker's agent inside of the victim enterprise. In phone phishing, an attacker sends email with a phone number for the victim to call or even leaves POTS voice mail with a recording asking the user to call back. The calls appear to go to a major U.S. or European bank, perhaps by using the area code of 212 associated with New York City. Attackers use VoIP technology with standard voice mail software to transfer the calls outside of the United States or Europe to a voice mail system located elsewhere; a friendly recorded voice then asks the user for confidential account information. Phone phishing is automated, telephone-based criminal social engineering on a worldwide scale. The attack and exploitation issues described in this section reinforce one another, allowing the attackers to dominate more "ground" for longer times in cyberspace, evading authorities and making money while doing so.

3.1.3 Social trends

Finally, we turn to the social trends that may result from changes in cyberspace. Social trends in the use and development of cyberspace include: worldwide technological development with different local emphases; rise in online communities, collaboration, and information-sharing.

- **Worldwide technological development, with different localized emphases**

Throughout the 1980s and much of the 1990s, the locus of cyberspace evolution was the United States and Europe. There, for example, the Internet originated with the Defense Advanced Research Projects Agency, many of its standards were developed by the Internet Engineering Task Force, and the World Wide Web standards were created at CERN in Geneva. Recently, however, the trend is toward more internationalization of cyberspace deployment and technological development. A large fraction of the planet's population is now online.[46] The Internet is, however, only one aspect of cyberspace: today, cell phones give more than two billion people the ability to tap into the world's telephony network. This lowers barriers to entry and allowed players from around the world to participate in cyberspace activities, for good or ill. While this trend is broad-based, various countries have carved out particular niches of their focus in cyberspace.[47]

The involvement of more countries in the advancement of global high-tech infrastructures means that covert monitoring and control capabilities for exploitation and disruption could be added at numerous points in the supply chain outside of the United States. These overall national areas of technological dominance are blurring with time. Some countries are making major investments in underlying bandwidth and tweaking incentives so they can become havens for high technology and new corporate development. Such activities have diminished the overall U.S. dominance of cyberspace as more and more significant contributions are made on a worldwide basis, not just by U.S.-based or European companies. Even U.S. - based companies, such as Microsoft and Google, are investing in research and development operations outside of the United States, particularly in China. Such a shift has significant intellectual property implications, as innovations devised outside of the United States by international corporations offer fewer avenues for U.S. control and increased control by other countries.

From an economic perspective, the U.S. tendency has been to rely generally on a broad free-market approach to technological development. Some other countries have relied on targeted incentives for specific technologies in an attempt to leap ahead of other players. These differing approaches have contributed to the trend of different emphases in various countries' technological development. The trend toward internationalization of cyberspace technological change is especially visible in the realm of computer and network attacks. In the 1990s, most attacks, and indeed almost all publicly released computer attack tools (both free and commercial), came from the United States or Europe.

In the early 2000s, however, computer attacks went international. Several widespread worms have been released by citizens of countries not commonly associated with high technology: in 2000, the Love Bug computer virus was released by a student in the Philippines, and in 2005, the Zotob bot was released by a developer from Morocco, funded by an individual from Turkey.[48] There have been plausible allegations of Chinese probing of cyberspace, including the highly publicized Titan Rain series of attacks against U.S. military facilities.[49] North Korea, not a typical bastion of computer technology, has boasted of its cyber war hacking abilities and is rumoured to run a hacking training program.[50] Not just attack tools but attacks themselves have taken on a more pronounced international flavour.

Two decades ago, the origin of most attacks across the public Internet was within the United States and Europe, usually a single spot. Attacks typically now come simultaneously from multiple countries, often a dozen or more. Some of these attacks are conducted by one individual in one location using bot-infected machines in other countries to mask the source of the attack, while other attacks are launched by coordinated attackers located in multiple countries. Attackers sometimes log in to U.S. systems from outside the country and use them as a base for attacks against other targets or for hosting propaganda. Some attackers motivated by geopolitical or nationalism issues launch an attack from one country against another hostile country, while others choose to launch an attack between friendly countries, hoping it will escape scrutiny. Thus, attacks sometimes come from Canada to the United States when the attackers themselves, located elsewhere, use the Canadian machines in an effort to blend in with normal traffic between the two allies.[50]

These trends are likely to continue, as broadband access, technical training and expertise, and high-technology industries spread. For decades, students from overseas received training in high technology at U.S. academic institutions, and many took their expertise back to their home countries. Recently, world-class high-technology universities have been established in India (including the Indian Institute of Technology) and China (with its University of Science and Technology of China); thus, many students worldwide now receive high-tech training indigenously. The gap between levels of technological skill in the United States or in Europe and those in the rest of the world is shrinking and will continue to do so. Of course, the United States and Europe will keep pushing ahead to new technologies, and their existing base is an advantage, but yesterday's gaps have significantly narrowed.

- **Rise in online communities, collaboration, and information-sharing**

Another major cyberspace trend is the rise in online communities made up of people or organizations with common interests who coordinate in cyberspace to share information and achieve other goals. As the term is most commonly used, an online community refers to a social setting in cyberspace, such as MySpace, LinkedIn, and Orkut, where consumers with common interests communicate and share personal profiles, business contacts, and so forth. Such sites have flourished recently; MySpace had over 300 million accounts for users around the world as of 2007. Such social online communities also yield information- and data-

mining opportunities to law enforcement, as users provide detailed information about their lives and their network of acquaintances.

Unfortunately, there have also been high-profile cases of stalkers misusing this information to target children. While today's specific most popular online communities might be a mere fad, the concept of online communities in the form of social networking sites is likely to be an enduring trend. Another type of community is the blog, an online diary where a writer shares information and commentary about politics, hobbies, or other interests. Most bloggers allow others to provide comments on their blog, resulting in a community of sorts. The blogosphere [51] is witnessing very rapid growth. Some blogs have become quite popular and have helped shape political debates and news stories.

Blogs will likely become more consequential as the distinction between the blogosphere and traditional news media blurs. Many major newspapers have started their own blogging operations, for example, or have hired bloggers to write content for the Internet and for printed media. Making use of social networking and blogging for a very different objective, terrorist organizations have also formulated online communities, to aid in fundraising, recruitment, propaganda, and command and control of their operations.[52] Some of these sites are available to the public, especially those associated with propaganda, fundraising, and communiqués from terrorist leadership, while other sites, containing more sensitive information about the organization, are available only to those specifically invited.

Another use of online communities involves integrated supply chains, in which a given manufacturer relies on a host of suppliers, who in turn rely on their own suppliers, distributed in countries around the world, the whole controlled through cyberspace. With an integrated supply chain, messages regarding inventory, capacity, and payment can be transferred quickly, allowing the manufacturer to cope more efficiently with changes in demand and possible disruptions to supply.

Dell Computer famously relies on integrated supply chains using Internet technology; many other companies are also heavy users of these technologies, including United Parcel Service and Wal-Mart.[53] Given the transnational nature of such supply chains, each individual country through which the chain passes has some form of cyber power over that chain, with the ability to tax, slow down, or even shut off a vital component of the chain. However, with the economic importance of these chains, and their corporate owners' ability to use cyberspace to reroute capacity and demand or to set up new chains rapidly, most countries will probably use some restraint in their exercise of such power. Online communities also encompass sites associated with consumer commerce, such as Amazon.com and eBay; these have created a lively interchange of buyers and sellers, with complex ranking, preference, and voting systems for products and providers.

Some online communities involve participants in even deeper immersion in the cyber world. An example is Second Life, a site run by Linden Research, which describes their

offering as a "3D online digital world imagined, created, and owned by its residents." Users of this community create their own avatars, or online representatives, to explore and alter the virtual reality space inside of the community and to create objects to use or buildings to inhabit. People meet, have relationships, and conduct business transactions inside of Second Life, which even has its own currency.[54] While Second Life is targeted at adults, a special area within the Second Life world is geared to teenagers. Another example, for children 5 to 10 years old, is an online world of game-playing and avatars called Webkinz created by the toy company Ganz; it, too, has its own digital economy. There are many other such communities.

4. Information Technology-Pros and Cons

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 happened in Eastern Europe and North Africa).[55] 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. Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways.[56] 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. In 2003 alone, malicious software caused damages of up to USD 17 billion.[57] By some estimates, revenues from cybercrime exceeded USD 100 billion in 2007[58] outstripping the illegal trade in drugs for the first time. Nearly 60 per cent of businesses in the United States believe that cybercrime is more costly to them than physical crime. These estimates clearly demonstrate the importance of protecting information infrastructures. Most of the above-mentioned attacks against computer infrastructure are not necessarily targeting critical infrastructure.

However, the malicious software "Stuxnet" that was discovered in 2010 underlines the threat of attacks focusing on critical infrastructure. The software, with more than 4000 functions,[59] focused on computer systems running software that is typically used to control critical infrastructure. Thus, information technology plays an important role in the world. Many changes have been occurring in society with the emergence and growth of IT. There are many advantages as well as disadvantages for information technology. They are enumerated below:

4.1 Advantages of Information Technology

Some of the major advantages of information technology are:

- **Globalization**

The new electronic independence re-creates the world in the image of a global village.[60] IT has not only brought the world closer together, but it has allowed the world's economy to become a single interdependent system. This means that one can not only share information quickly and efficiently, but can also bring down barriers of linguistic and geographic boundaries. The world has developed into a global village due to the help of information technology allowing countries like Chile and Japan who are not only separated by distance but also by language to shares ideas and information with each other.

- **Communication**

With the help of information technology, communication has also become cheaper, quicker, and more efficient. One can now communicate with anyone around the globe by simply text messaging them or sending them an email for an almost instantaneous response. The internet has also opened up face to face direct communication from different parts of the world through video conferencing.

- **Cost effectiveness**

Information technology has helped to computerize the business process thus streamlining businesses to make them extremely cost effective money making machines. This in turn increases productivity which ultimately gives rise to profits that means better pay and less strenuous working conditions. Only few years ago there was no way to send free message through to the phone, but now people uses social network for free communication e.g. Viber, Skype, Facebook. Saving time and money for petrol as people can go shopping from home through online shopping.

- **Bridging the cultural gap**

Information technology has helped to bridge the cultural gap by helping people from different cultures to communicate with one another, and allow for the exchange of views and ideas, thus increasing awareness and reducing prejudice.

- **Absence of time restrictions**

IT has made it possible for businesses to be open 24 x 7 all over the globe. This means that a business can be open anytime anywhere, making purchases from different countries

easier and more convenient. It also means that one can have his goods delivered right to his doorstep with having to move a single muscle.

- **Creation of new jobs**

Probably the best advantage of information technology is the creation of new and interesting jobs. Computer programmers, Systems analyzers, Hardware and Software developers and Web designers are just some of the many new employment opportunities created with the help of IT.

- **Protecting and storing information**

Electronic storage systems are being created to hold the information that is being shared over the internet and internal intranets. Secure maintenance of customer and company files is vital to the integrity of the company. Virtual vaults keep information safe by limiting access to a select few. Security systems are put in place to protect your electronic information and keep it from being wiped out or damaged during a system breakdown. Hackers are also kept at bay with intense securities.

- **Automated processes**

The ability to find ways to complete more work in a shorter amount of time is essential to the success of a company. Information technology improves a company's efficiency by implementing automated processes to make employees more capable of handling a larger work load. Reports, queries and monitoring financials can be completed by the computer programs, leaving employees free to complete other tasks.

- **Education**

There is new opportunity for further education to improve qualification in so many economic sectors. A degree can be completed online from person's home. It is possible to hold a job and still do degree.

- **Remote access or telecommuting**

When a company has implemented an information technology system, many times employees can then access the company's network electronically. This enables employees to work from home or while on the road. This gives the employees more flexibility and they are more productive because they can still work when not in the office.

4.2 Disadvantages of Information Technology

Some of the major disadvantages of information technology are:

- **Expense of implementation and maintenance**

Setup costs for implementing an information technology system within a home or business can be very costly. Software can training can also take another big bite out of the budget. Information technology systems, just like any other equipment, need to be maintained and repaired from time to time. But there are also updating and upgrading costs associated with IT systems.

- **Unemployment**

While information technology may have streamlined the business process it has also created job redundancies, downsizing and outsourcing. This means that a lot of lower and middle level jobs have been done away with causing more people to become unemployed.

- **Violation of Privacy**

Though information technology may have made communication quicker, easier and more convenient, it has also bought along privacy issues. From cell phone signal interceptions to email hacking, people are now worried about their once private information becoming public knowledge.

- **Lack of job security**

Industry experts believe that the internet has made job security a big issue as since technology keeps on changing with each day. This means that one has to be in a constant learning mode, if he or she wishes for their job to be secure.

- **Dominant culture**

While information technology may have made the world a global village, it has also contributed to one culture dominating another weaker one. For example, it is now argued that US influences how most young teenagers all over the world now act, dress and behaviour. Languages too have become overshadowed, with English becoming the primary mode of communication for business and everything else.

- **Problems relating to social media**

The network pages are open to everyone including teenagers and young children which can affect their mental and physical health by watching and playing violent games. They became addicted to the phones, iPod, gaming consoles forgetting about outside activities and communication in the society.

- **Cyber bulling and other cyber wrongs**

It is so easy now bullying and threatening others in social network pages that this has become much easier for internet users all over the world. They don't realize what the consequences are to those reading/hearing unpleasant comments. In the recent past there have been so many investigation cases regarding cyber bullying with lethal consequences.

- **Undue reliance on technology**

People don't bother to read, calculate or write without computers anymore in same time losing abilities of hand writing (why write if can use spell-checker), calculate without calculator even for minor addition, reading books (why read if there so much information in internet).

4.3 Information technology *vis-a-vis* children's development

Information-communication technologies (ICT) can be very attractive and child-friendly for pre-school children, who acquaint with them very quickly.[61] As seen earlier, the broad definition of ICT encompasses a variety of everyday technologies like electronic toys, interactive whiteboards, playing consoles, various players and digital cameras- all types of technology that a child may encounter in its home environment and also uses them.

Besides using ICT for pleasure and entertainment; it is also used for study and work purposes.[62] ICT encourages learning; it motivates the individual and gives him the capability to do certain activities. Its presence betters the learning environment and enriches the learning experience.[63] ICT enables the child to process the learning content in an entertaining and interesting way. ICT also develops the child's competences.[64] ICT is not only an educational tool, but also a supporting one, because it helps to develop children with special needs and behavioural problems.[65] It also lays the foundation for long life learning and personal development, because *inter-alia* it develops the digital competence and technical competences, which are needed for employment, education, self-development, and general activeness in the modern society.

For many years ICT have been judged for its potentially negative influence on the child. Often, worries about its usage are concerned with the question how early exposing of the child to the ICT influences its general development. Certain experts claim that the children learn more from real life experiences than from the ones offered by ICT, especially if the content is not suitable for the children.[66] The debate about the technology's influence on the child's development has long ago exceeded the borders of academic circle and became public. Some scholars have found out that even the general public thinks that the usage of ICT is dangerous for the child, and that its creative potential is being more and more overlooked.[67] The major argument of all studies, which stress the negative sides of ICT is that the children in early stages of development are the most susceptible and because of that also very vulnerable.

One of the studies divided the dangers and disadvantages of ICT usage into three major categories:[68]

(i) That includes dangers and disadvantages of its usage for the child's socio-cultural development. The writers found out that ICT supposedly endangers the child's social development, because children spend less time playing with their peers and are mostly isolated; ICT is supposedly to offer virtual experiences from "the second hand" and not realistic experiences from "the first hand."

(ii) That includes the dangers and disadvantages of ICT usage for the child's cognitive development. ICT is supposedly to endanger the child's intellectual development, the development of imagination (it stimulates passivity and not activity), and the development of language (lack of communication with peers).

(iii) That includes dangers and disadvantages of ICT usage for the child's wellbeing. Children are supposedly to spent more time in enclosed spaces and not outdoors, the child's health is also endangered (sitting usage, which increases the risk of obesity), the usage of ICT supposedly leads to addiction with technology and exposure to inappropriate content., besides all that the chances of child interacting with family members are also decreased, what is supposedly to lead towards decreasing of child's emotional development.

All these dangers and disadvantages are mostly connected with the amount of ICT usage, its content and the degree of parent control. Today, children can through ICT more easily access various contents than ever before. Adults do not have control over this access, because the media environment has changed so drastically that a complete control over the child's usage of ICT is today practically impossible.[69]

Parents believe that the most common negative consequences are: contact with aggressive or unsuitable content, endangerment of the physical health (deterioration of sight, stiffness, spinal injuries because of constant sitting position, obesity), associability, and loss of constant with reality or even addiction. Besides that they also emphasise the positive consequences which are: gaining new knowledge and skills, knowing the ICT what will benefit the child in its future schooling and employment. Those parents, who think that the usage of ICT is more harmful than beneficial for their child, argue their opinions by claiming that a child is too young to use the ICT. They are also afraid that the usage of ICT increases the chances of serious problems in the child's mental development, that the child will become aggressive, that it will lack social interaction (isolation from society) and that its communicational skills will be worsened. Only a few parents believe that ICT has positive effects on a child.

A study has found out that, children on average use ICT between one and three hours per day.[70] This usage often goes on without the parents' approval, because children have unlimited access to their own, personal media. At the age of four the child is already in the potential danger, if the usage of ICT is not correctly regulated. Because of that parents have to provide the control and consistently execute it. There is a need for balance between all

children's activities, there have to be timelines, there has to be an equal distribution between child's play indoors and outdoors, and between individual and group play. The question how often and how much the child uses ICT has always arouse great differences in experts' opinions. Some of them believe that the usage of ICT harms the child, while others see only positive effects in its usage.

4.4 Impact of Information Technology on organizations and corporate world

Information technology is very the backbone of the Indian economy. It expels the many different technologies inherent in the field of information technology and their impact on information systems to the collection of tools that make it easier to use, create, manage and exchange information. The Internet is the latest of a long series of information technologies, which includes printing, mail, radio, television and the telephone. Information Technology Services is to provide an innovative, customer-focused, and robust foundation for information technology solutions that enable the university community to pursue excellence in research, education, and public service. [71]

Information Technology Services seeks to establish trust with customers through professionalism, honest and open dialogue, high quality customer service, and a commitment to partnership and collaboration. In the backdrop of all these developments, the present section makes an attempt to: expels with the various roles, advantages and disadvantages those are being followed in present scenario in information technology.[72]

Information Technology covers a broad spectrum of hardware and software solutions that enable organizations to gather, organize, and analyze data that helps them achieve their goals. It also details technology-based workflow processes that expand the capacity of an organization to deliver services that generate revenue. The four main focuses of IT personnel are: (i) business computer network and database management; (ii) information security; (iii) business software development; and (iv) computer tech support. As the IT industry evolves to meet the technology demands of today's workplace, different challenges are arising and IT professionals are striving to meet them. Network security is by far the greatest concern for many companies and they rely on their IT staff to prevent or stop these system breaches.[73]

Data overload is becoming an increasingly important issue since many businesses are processing large amounts of data on a daily basis; with many of them not have the processing power to do so. Last, but not least, two of the most essential skills needed from IT professionals are teamwork and communication skills. Systems are complex and people are needed to help translate that task. Therefore, IT professionals are the ones responsible for helping others get their work done efficiently without the complex jargon of the technology world.

Some of the most popular positions in Information Technology are:

- **IT Manager**

They are the contact persons when one's email would not send or Microsoft Word does not open. As the head of the IT department, they ensure that a company's network is operating smoothly and that dangerous threats like malware are minimized.

- **Computer Systems Analyst**

Analysts design and develop computer systems and are an expert at every facet of hardware, software, and network. They also evaluate the systems and research the industry for better products to enhance their existing system.

- **Health IT Specialist**

Health IT is booming, especially with the transition from paper to electronic health records. Health IT specialists will mix computer knowledge will record-keeping skills, medical coding, and billing.

- **Web Developer**

Web developers are in high demand because they have a great understanding of what makes a good operating system. They create web pages, web applications and web content with their knowledge of what the average surfer finds visually stimulating and how to optimize sites for mobile tech, among numerous other skills. [74]

- **Cloud Specialist**

Cloud specialists organize and give configuration to the information infrastructure in the sky. Because this is still an emerging technology, these architects are highly sought after and one of the top-paying professions in the industry.

- **Computer Forensic Investigator**

These investigators are computer crime detectives that search for, identify, and evaluate information from computer systems.

- **Database Administrator**

Database administrators create, upgrade, and test for databases.

- **Information Technology Vendor Manager**

Slightly more hands-off compared to some tech positions, vendor managers oversee supply when it comes to software and hardware. This can mean anything from Microsoft's latest word processor to health IT programs for hospitals.

- **Computer Systems Administrator**

The expertise of network and computer systems administrators is essential to every office. Aside from maintaining a healthy computer network, they also lend their tech knowledge to managing telecommunication networks.

- **Mobile Application Developer**

Because of the highly-mobile lifestyle, mobile application developers are and will be in high demand for years to come, especially as mobile devices and technology becomes increasingly sophisticated.

Information technology has become a vital and integral part of every business plan. From multi-national corporations who maintain mainframe systems and databases to small businesses that own a single computer, IT plays a role. The reasons for the omnipresent use of computer technology in business can best be determined by looking at how it is being used across the business world.

✓ **Communication**

For many companies, email is the principal means of communication between employees, suppliers and customers. Email was one of the early drivers of the Internet, providing a simple and inexpensive means to communicate. Over the years, a number of other communications tools have also evolved, allowing staff to communicate using live chat systems, online meeting tools and video-conferencing systems. Voice over internet protocol (VOIP) telephones and smart-phones offer even more high-tech ways for employees to communicate.

✓ **Inventory management**

When it comes to managing inventory, organizations need to maintain enough stock to meet demand without investing in more than they require. Inventory management systems track the quantity of each item a company maintains, triggering an order of additional stock when the quantities fall below a pre-determined amount. These systems are best used when the inventory management system is connected to the point-of-sale (POS) system. The POS system ensures that each time an item is sold, one of those items is removed from the inventory count, creating a closed information loop between all departments.

✓ **Data management**

The days of large file rooms, rows of filing cabinets and the mailing of documents is fading fast. Today, most companies store digital versions of documents on servers and storage devices. These documents become instantly available to everyone in the company, regardless of their geographical location. Companies are able to store and maintain a tremendous amount of historical data economically, and employees benefit from immediate access to the documents they need.

✓ **Management Information Systems (MIS)**

Storing data is only a benefit if that data can be used effectively. Progressive companies use that data as part of their strategic planning process as well as the tactical execution of that strategy. Management Information Systems enable companies to track sales data, expenses and productivity levels. The information can be used to track profitability over time, maximize return on investment and identify areas of improvement. Managers can track sales on a daily basis, allowing them to immediately react to lower-than-expected numbers by boosting employee productivity or reducing the cost of an item.

✓ **Customer Relationship Management (CRM)**

Companies are using IT to improve the way they design and manage customer relationships. Customer Relationship Management systems capture every interaction a company has with a customer, so that a more enriching experience is possible. If a customer calls a call centre with an issue, the customer support representative will be able to see what the customer has purchased, view shipping information, call up the training manual for that item and effectively respond to the issue. The entire interaction is stored in the CRM system, ready to be recalled if the customer calls again. The customer has a better, more focused experience and the company benefits from improved productivity

5. Summary and Conclusion.

The future of cyberspace is likely to involve the embedding of Internet and personal computer technology deeply into many everyday objects, including not only technical items such as computers, telephones, radios, and televisions, but also items not now associated with cyberspace, such as home appliances, consumer products, clothing, and more. These everyday objects will incorporate software intelligence, processing information delivered wirelessly by a broadband connection. Global positioning systems (GPS) and RFID tags will allow these everyday objects to locate and interact with each other in the physical world. Cars, ships, airplanes, weapons systems, and their components will all become more intelligent and interactive, increasingly without direct human control. The economies of developed nations will rely on this interconnected grid of objects. Unfortunately, however, the grid is built on technologies not consciously designed to handle information of such an extent and value. Security flaws will let attackers establish widespread collections of infected objects they can use to exploit other objects, manipulate target organizations, and possibly disrupt countries and economies. Such actions are not at all far-fetched, based on the accumulated evolutionary trends of the past decade. Revolutionary changes could have an even unexpected impact on cyberspace.

6. Bibliography

1. *Ottis, R. & Lorents, Cyberspace: Definition and Implications (Academic Publishing Limited, 2010), pp 267-270; see also, Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April (2010).*
2. *William Gibson quoted in Cotton and Oliver, 1994, p.54.*

3. *Rebecca Bryant, "What Kind of Space is Cyberspace?" 5 Minerva - An Internet Journal of Philosophy 138-155 (2001)*
4. *ITU, National Cyber Security Strategy Guide (2011); See also, Schatz, Daniel; Bashroush, Rabih; and Wall, Julie, "Towards a More Representative Definition of Cyber Security,"12 (2) Journal of Digital Forensics, Security and Law 53-74 (2017)*
5. *ITU-T X.1205: Overview of Cyber Security- ITU-T Recommendations, X Series: Data Networks, Open System Communications and Security (2008)*
6. *Hathaway M, Klimburg, "Preliminary Considerations: On National Cyber Security" in Klimburg A (ed), National Cyber Security Framework Manual (NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2012)*
7. *Tuija Kuusisto & Rauno Kuusisto, "Cyber World as a Social System" in Lehto & Neittaanmäki (eds.), Cyber Security: Analytics, Technology and Automation, Intelligent Systems, Control and Automation: Science and Engineering 31-43 (Springer International Publishing Switzerland)*
8. *The Oxford English Dictionary, (2009 Edition)*
9. *National Security Presidential Directive 54/Homeland Security Presidential Directive 23, (2008)*
10. *New Zealand Cyber Security Strategy, 2011*
11. *Cyber Security Strategy for Germany, 2011*
12. *Canada's Cyber Security Strategy, 2010*
13. *See "Cyber Power and National Security: Policy Recommendations for a Strategic Framework," in FD Kramer, S. Starr, L.K. Wentz (ed.), Cyber Power and National Security, (National Defense University Press, Washington, 2009)*
14. *Definition by Marco Mayer, Luigi Martino, Pablo Mazurier and Gergana Tzvetkova, Draft Pisa, 19 May 2014*
15. *Do D Joint Publication 3-12(R) Cyberspace Operations (5 February 2013).*
16. *Kunstkritikk, The (Re) invention of Cyberspace (2015).*
17. *Choucri, Nazli, "Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences" (October 13, 2014). MIT Political Science Department Research Paper No. 2014-29.*
18. *Gibson, W., Neuromancer (USA: Ace Books, 1986)*
19. *Edward Skoudis, "Evolutionary Trends in Cyberspace" https://pdfs.semanticscholar.org*
20. *Intel Corporation, "Moore's Law," available at www.intel.com*
21. *Bob Briscoe, Andrew Odlyzko & Benjamin Tilly, "Metcalfe's Law Is Wrong," IEEE Spectrum (July 2006)*
22. *International Telecommunication Union, Broadband Penetration by Technology, Top 20 Countries Worldwide (2004).*
23. *"What is the Speed of Standard Data Rates?" Whatis.com, http://whatis.techtarget.com.*
24. *Google, Amazon, eBay, and Microsoft.*
25. *Net neutrality issues are being studied by Japan's Ministry of Internal Affairs and Communications to determine a reasonable balance among the competing factors. The European Union has tentatively supported neutral networks, but companies such as Deutsche Telekom and Telecom Italia are beginning to lobby for changes to the existing European approach. A Net neutrality Bill in the U.S. Congress require ISPs to handle traffic independently of their business relationships. Such legislation is hotly contested, and it is not yet clear how the issue will evolve.*

26. *Rioters in France in late 2005 and early 2006, people involved in Ukraine's Orange Revolution in the winter of 2004/2005, and terrorist organizations have all relied on cheap and ubiquitous cell phone text-messaging to exercise command and control and to disseminate information.*
27. *For instance, stores in shopping malls use wireless for point-of-sales terminals and inventory control, and military deployments can rapidly deploy computer networks.*
28. *Although it has a maximum throughput of 70 Mbps and a maximum distance of 70 miles, WiMAX in real-world circumstances achieves approximately 10 Mbps over about 2 miles.*
29. *Several organizations have expressed interest in using RFID technology for large-scale inventory management, including Wal-Mart Corporation, the U.S. military, and the Chinese government. The U.S. State Department has begun using RFID tags in electronic passports.*
30. *For example, the Internet Protocol Security (IPsec) specification was designed to be mandatory in IPv6.*
31. *Including Cisco and Microsoft, whose products support the protocol*
32. *Although IPsec is mandatory in IPv6; it does not necessarily mean that the newer protocol will immediately boost security. To speed and simplify deployment, users sometimes implement IPv6with IPSec without the necessary trusted encryption keys, in effect blindly trusting any system on the network. Some IPv6 implementations use blank ciphers, leaving data unencrypted. Such deployments nullify any authentication and confidentiality benefits of IPsec within IPv6. Even with the careful use of trustworthy keys and ciphers, systems supporting IPv6 may still have a large number of security flaws, at least initially, in their protocol stacks. These could allow for remote denial-of service attacks that cause a system crash or that exhaust all processing or memory resources, or they could permit system compromise and control by an attacker.*
33. *This phenomenon is sometimes referred to as Wirth's law, named after Niklaus Wirth, a Swiss computer scientist and inventor of Pascal and several other programming languages. Wirth's law states that software is decelerating faster than hardware is accelerating.*
34. *In an example of search directives, Google's "file type:" allows a search for specific types of files: Microsoft Excel spreadsheets, where "file type: xls" is a search term, or MS Word documents, if a search includes file type: doc, while "site:" limits search results to a given Web site. An operator such as "-" (NOT) filters out all Web pages with a given term; using the operator "AND" allows a search limited to results containing both of the terms on either side of the operator.*
35. *Honey pots are used to detect attacks, research attackers' motives and methods, and provide a limited environment, isolated from critical facilities, in which to engage attackers. Given VMEs' ability to reset an infected system quickly, most malicious code researchers utilize them to analyze the capabilities of the latest malware and to construct defences. If a malware specimen under analysis infects and damages a guest virtual machine, the VME lets a researcher revert to the last good virtual machine image, quickly and easily removing all effects of the malware without having to reinstall the operating system.*
36. *Rich Gordon, "Convergence Defined," USC Annenberg Online Journalism Review: www.ojr.org.*
37. *John Borland, "iTunes Outsells Traditional Music Stores," CNET News, (November 2005)*
38. *For example, ABC's most popular shows*

39. *For example, YouTube, Google etc*
40. *Marshall Kirkpatrick, "YouTube Serves 100m Videos Each Day," TechCrunch, (July 2006)*
41. *For example, if an enterprise's Internet connection goes down, most users will expect to be unable to get email, but in some enterprises, critical business functionality might also become inaccessible if it depends on Web applications residing on third-party servers on the Internet.*
42. *Typically, Windows, variations of UNIX and Linux, or Cisco's Internetwork Operating System*
43. *In the United States, the older system was dominated by the Regional Bell Operating Companies and their parent company, AT&T, which provided this stewardship under significant Federal, state, and even local regulatory control that constrained the rates they could charge for service and set standards for service reliability.*
44. *Spam comprised about 30 percent of all email in 2003, has gone to over 80 percent today, and continues to rise.*
45. *A single infected machine displaying pop-up ads, customizing search engine results, and intercepting keystrokes for financial accounts could net an attacker $1 per month or more. A keystroke logger on an infected machine could help the attacker gather credit card numbers and make $1,000 or more from that victim before the fraud is discovered. With control of 10,000 machines, an attacker could set up a solid profit flow from cyber crime.*
46. *Even one decade ago, over one billion people had at least rudimentary access to the Internet. See, Mini Watts Marketing Group, World Internet Usage and Population Status (2007)*
47. *For example, China has aggressively moved into manufacturing computers, network equipment, and telecommunications infrastructure and devices. India offers various services using the distribution media of the Internet, including call centre support, software development, tax preparation, and other knowledge-based services. Europe, South Korea, and the United States have widespread broad- band access and major software development, both by commercial companies and open-source initiatives. Europe has been particularly strong in cell phone development and Japan in hand-held gadgetry such as games, digital cameras, and video players. A typical computer, network router, or operating system involves hardware and software assembled from several countries; the true source of given components may be difficult or impossible to track down.*
48. *Robert Lemos, "Zotob Suspects Arrested in Turkey and Morocco," Security Focus (August 2005)*
49. *Nathan Thornburgh, "Inside the Chinese Hack Attack," Time, (August 25, 2005)*
50. *Brian McWilliams, "North Korea's School for Hackers," Wired, (June 2003)*
51. *As all of the blogs on the Internet are collectively known*
52. *United States Institute of Peace, "www.terror.net: How Modern Terrorists Use the Internet," (March 2004)*
53. *Thomas L. Friedman, The World is Flat: A Brief History of the 21st Century (New York: Farrar, Straus and Giroux, 2005)*
54. *"Linden Dollars" can be bought and sold in the online community using U.S. dollars*
55. *Barney, Prometheus Wired: The Hope for Democracy in the Age of Network Technology (2001); White, "Citizen Electronic: Marx and Gilder on Information Technology and Democracy" 1 Journal of Information Technology Impact, 20 (1999)*

56. *Wilshusen, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, (GAO Document GAO-08-212T, 2007)*
57. *CRS Report for Congress on the Economic Impact of Cyber-Attacks, (April 2004), p. 10*
58. *O'Connell, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, (17.10.2007)*
59. *American Gas Association, Cyber Security Communique (2010)*
60. *Mc Luhan, M, Understanding Media: The Extensions of Man (McGraw-Hill, 1964)*
61. *Jurka Lepičnik-Vodopivec & Pija Samec, "Advantages And Disadvantages of Information-Communication Technology Usage for Four-Year-Old Children, and the Consequences of its Usage for the Children's Development" 2 (3) International Journal of Humanities and Social Science 54-57 (2012)*
62. *Punie, Y., "Learning Spaces: An ICT-enabled Model of Future Learning in the Knowledge-based Societyz" European Journal of Education, 42 (2007) http://onlinelibrary.wiley.com*
63. *Markovac, V. & Rogulja, N., Key ICT Competences of Kindergarten Teachers (Faculty of Education, University of Zagreb, 2009), pp. 72-77*
64. *Mc Pake, Stephen, Plowman, Sime & Downey, Already at a Disadvantage? ICT in the Home and Children's Preparation for Primary school (University of Stirling,2005): http://www.ioe.stir.ac.uk*
65. *Jitender K Malik, the criminals in a cyber environment using computer networks, International Journal of Current Innovation Research, Vol. 4, Issue, 12(A), December, 2018, pp. 1416-1422,*
66. *Kirkorian, Wartella & Anderson, "Media and Young Children's Learning" 18 Future of Children, 39-61 (2009)*
67. *Plowman, McPake & Stephen, "Just picking it up? Young Children Learning with Technology at Home" 38 Cambridge Journal of Education, 303-319 (2008)*
68. *Plowman, McPake & Stephen, "The Technologization of Childhood? Young Children and Technology in the Home"Children and Society, 24(2010)*
69. *Roberts, Foehr, Rideout, and Brodie, "Kids and Media @ the New Millennium" http://www.kff.org.*
70. *Jitender Kumar Malik and Sanjaya Choudhury, PolicyXZ. International Journal of Recent Scientific Research, Vol. 9, issue 12(A) , December, 2018, pp. 29811-29814.*
71. *Kling, R., McKim, G., & King, A, "A Bit more to it: Scholarly Communication Forums as Socio-technical Interaction Networks 54(1) Journal of the American Society for Information Science and Technology, 47-67 (2003).*
72. *Prasanna Kumar, "Information Technology: Roles, Advantages and Disadvantages" 4 (6) International Journal of Advanced Research in Computer Science and Software Engineering 1020-1024 (June 2014)*
73. *Garvey, W. D, Communication, and the Essence of Science: Facilitating Information Exchange among Librarians, Scientists, Engineers, and Students (New York: Pergamon Press. 1979)*
74. *Jitender k malik, cyber-crimes- policy in India, International Research Journal of Human Resources and Social Sciences, Volume 5, Issue 04, April 2018, 554-565.*