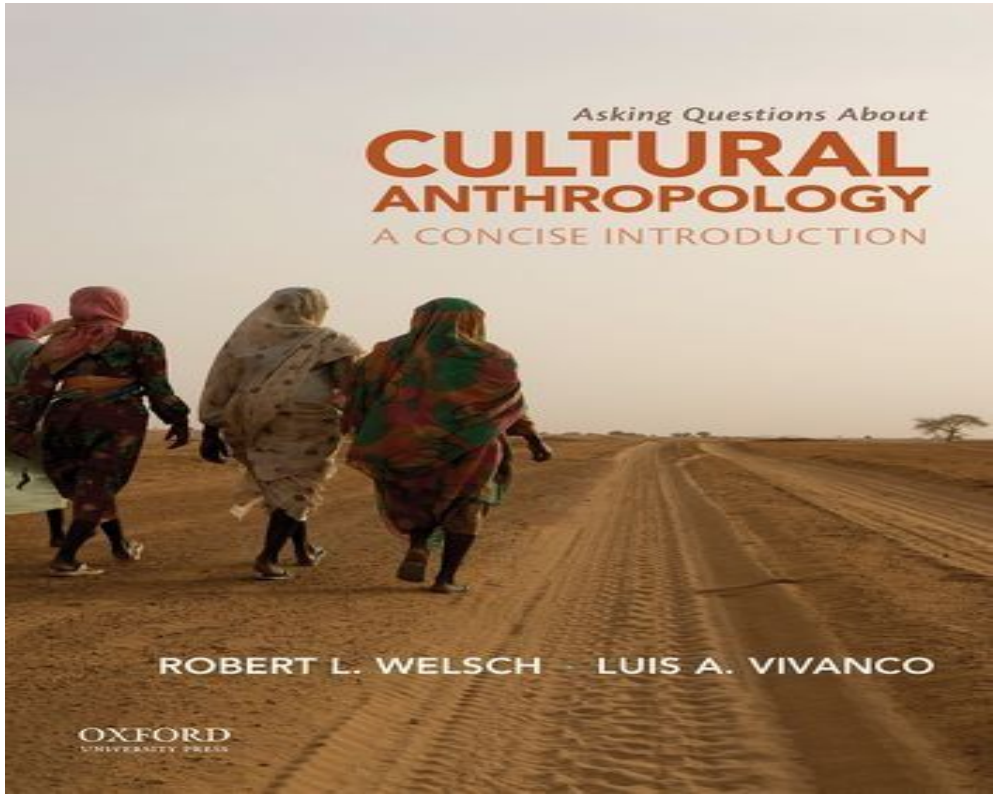
Cyberculture- An Anthropological Perspective

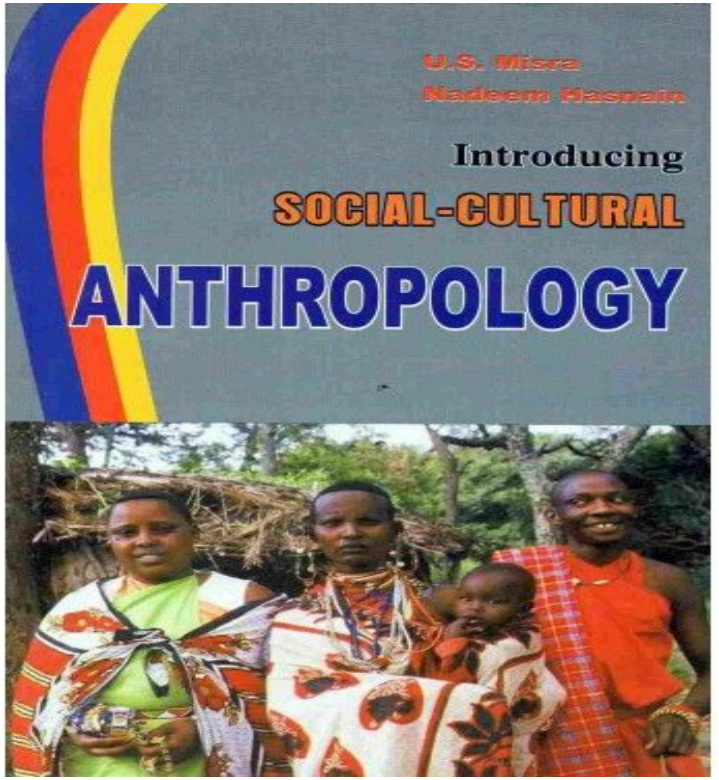
DR. BARNALI CHETIA

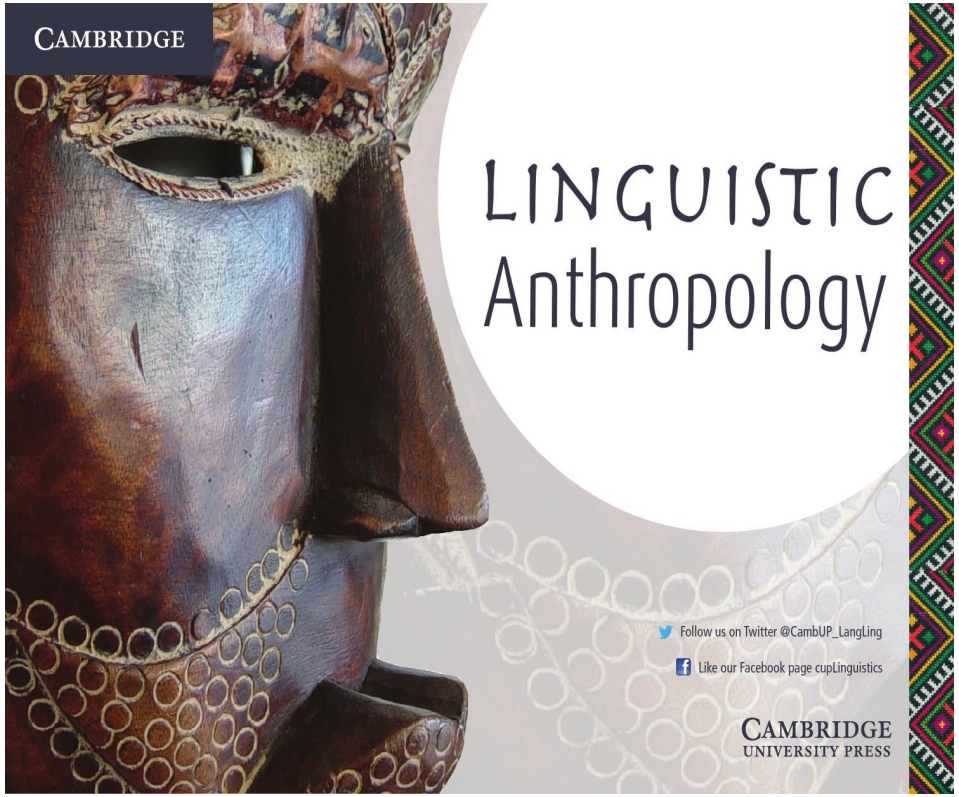
Introduction

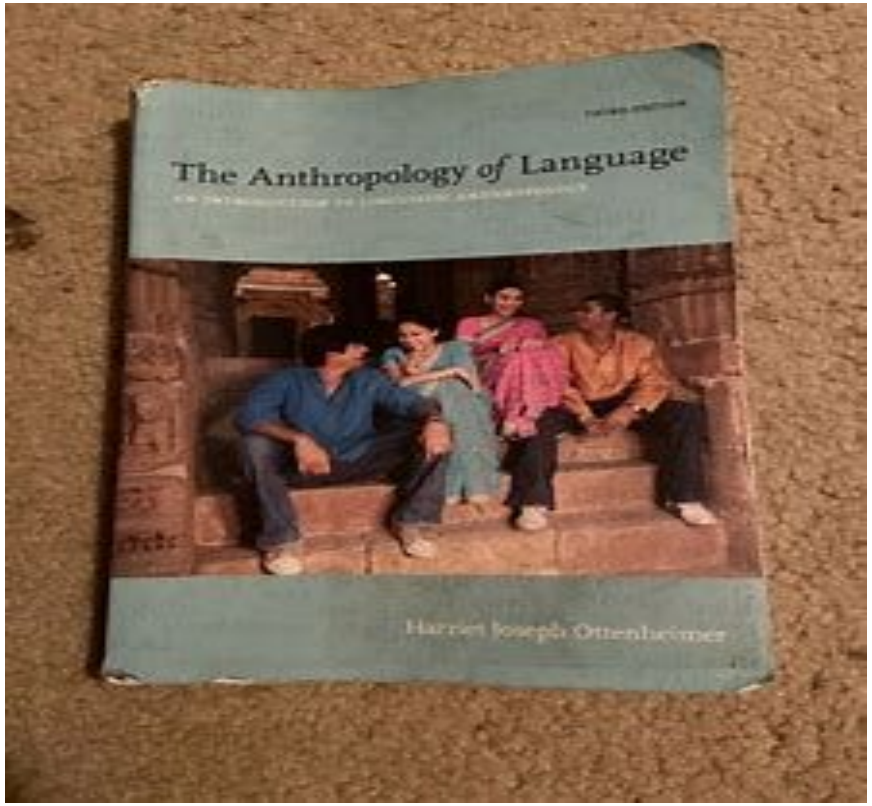
- **Anthropology** is the scientific study of humans (humanity), concerned with human behavior, human biology, cultures and societies, in both the present and past, including past human species.
- Social anthropology studies patterns of behaviour, while cultural anthropology studies cultural meaning, including norms and values.
- Linguistic anthropology studies how language influences social life.
- Biological or physical anthropology studies the biological development of humans.
- Visual anthropology, which is usually considered to be a part of social anthropology, can mean both ethnographic film (where photography, film, and new media are used for study) as well as the study of "visuals", including art, visual images, cinema etc.

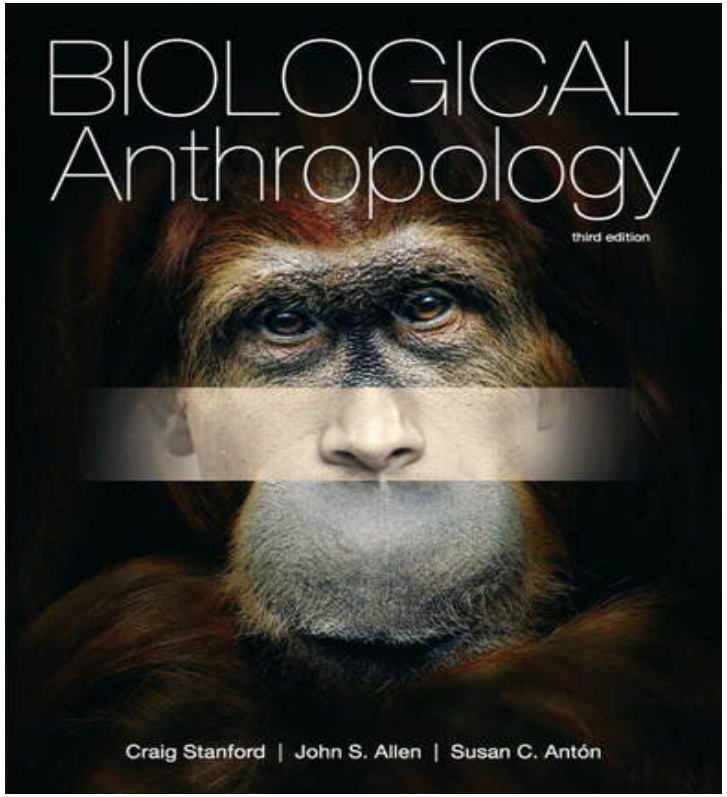
Biological or Physical Anthropology

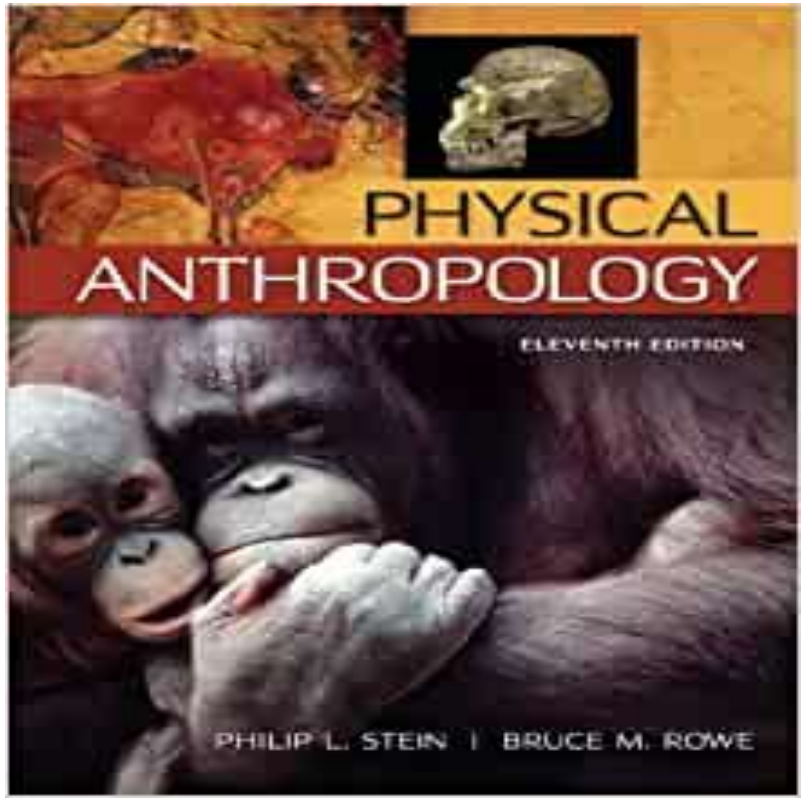

Asking Questions About
CULTURAL
ANTHROPOLOGY
A CONCISE INTRODUCTION
ROBERT L. WELSCH
LUIS A. VIVANCO
OXFORD

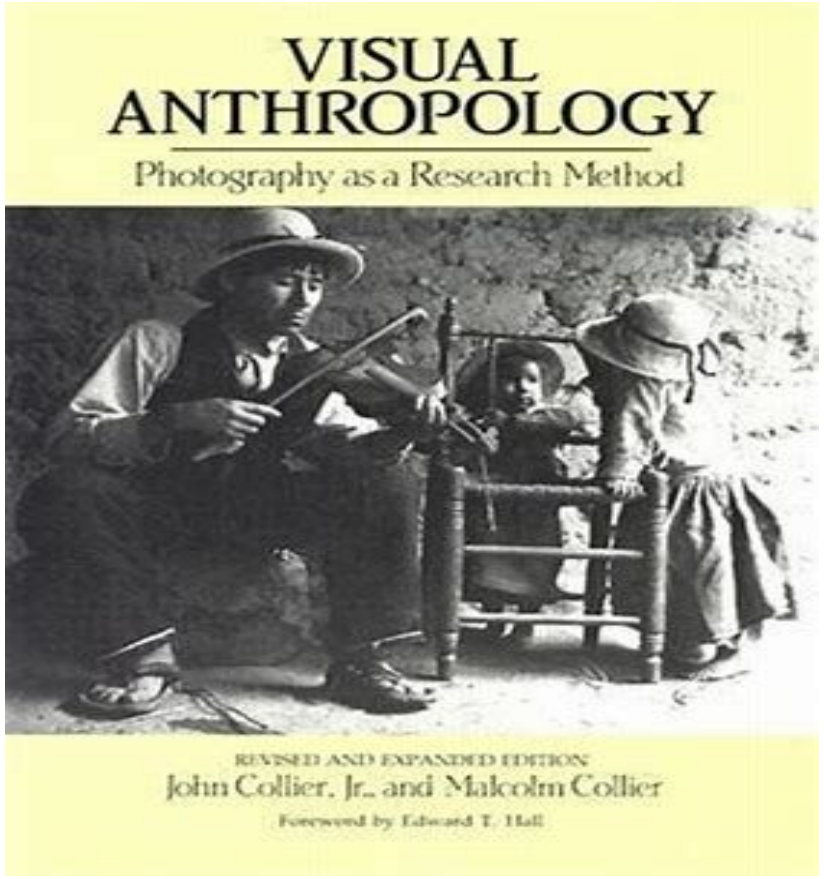

U.S. Misra
Nadeem Hasnain
Introducing
SOCIAL-CULTURAL
ANTHROPOLOGY

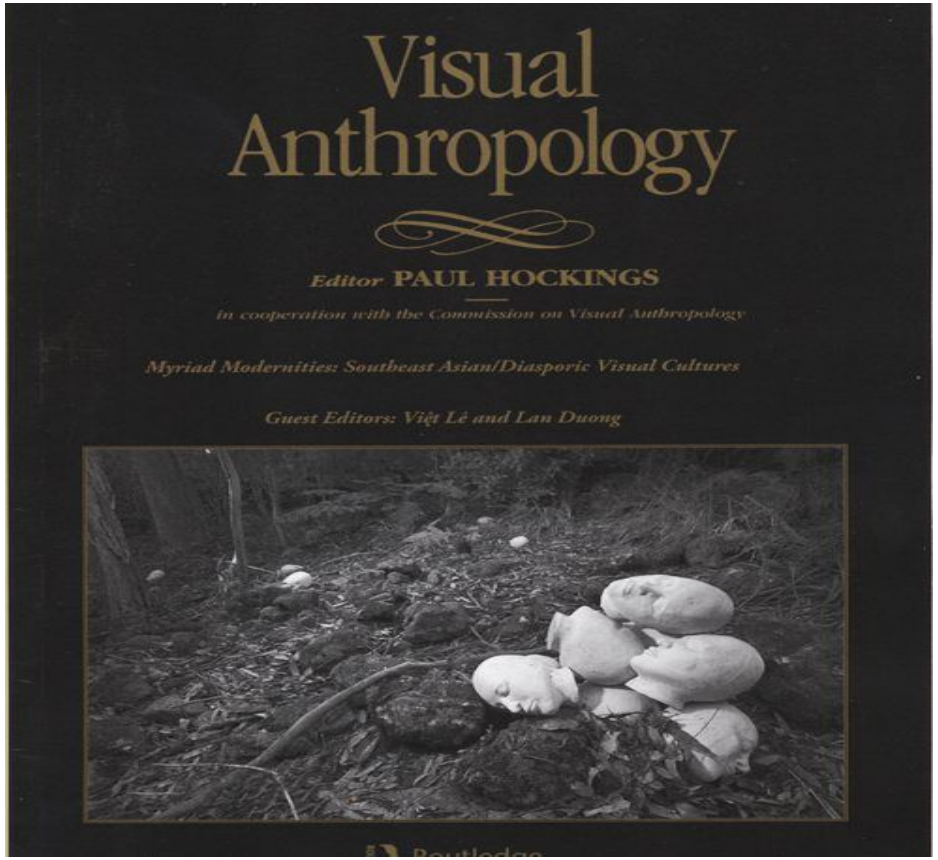

CAMBRIDGE
LINGUISTIC
Anthropology
Follow us on Twitter @CambUP_LangLing
Like our Facebook page cupLinguistics
CAMBRIDGE
UNIVERSITY PRESS

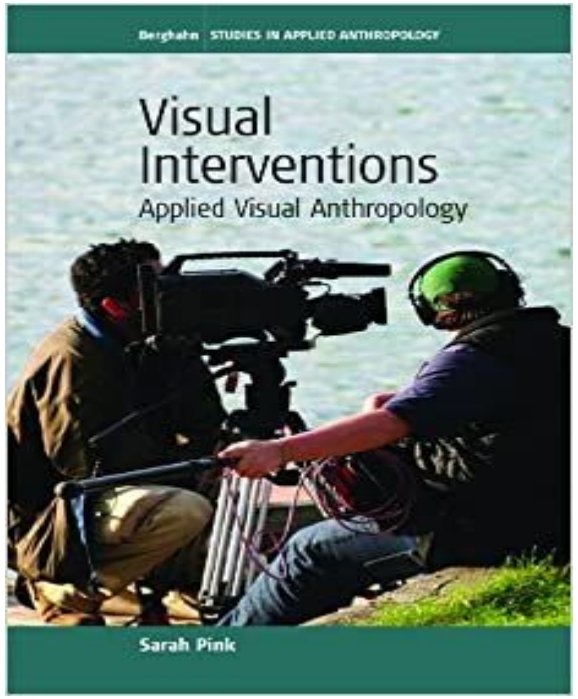

The Anthropology of Language


BIOLOGICAL
Anthropology
third edition
Craig Stanford | John S. Allen | Susan C. Antón


PHYSICAL
ANTHROPOLOGY
ELEVENTH EDITION
PHILIP L. STEIN | BRUCE M. ROWE


VISUAL
ANTHROPOLOGY
Photography as a Research Method
REVISED AND EXPANDED EDITION
John Collier, Jr., and Malcolm Collier
Foreword by Edward T. Hall


Visual
Anthropology
Editor PAUL HOCKINGS
in cooperation with the Commission on Visual Anthropology
Myriad Modernities: Southeast Asian/Diasporic Visual Cultures
Guest Editors: Việt Lê and Lan Duong


Berghahn STUDIES IN APPLIED ANTHROPOLOGY
Visual Interventions
Applied Visual Anthropology
Sarah Pink


Westfälische Wilhelms-Universität Münster
› New Master Program:
Visual Anthropology, Media & Documentary Practices
Apply now for this Master of Arts at the University of Münster in Germany!
› Advanced training course option: all classes can be booked separately.
www.wwu-weiterbildung.de/anthropology
living.knowledge
WWU Münster
WWU
Weiterbildung

- The Word ‘culture’ comes from the Latin word ‘cultura,’ related to cult or worship. In its broadest sense, the term refers to the result of human interaction.
- Society’s culture comprises the shared values, understandings, assumptions, and goals that are learned from earlier generations, imposed by present members of society, and passed on to succeeding generations.
- Sometimes an individual is described as a highly cultured person, meaning that the person in question has certain features such as his/her speech, manner, and taste for literature, music, or painting, which distinguish him/her from others.
- Culture, in this sense, refers to certain personal characteristics of an individual.

- However, this is not the sense in which the word culture is used and understood in social sciences.
- Sometimes culture is used in popular discourse to refer to a celebration or an evening of entertainment, as when one speaks of a ‘cultural show.’ In this sense, culture is identified with aesthetics or the fine arts such as dance, music, or drama.
- This is also different from the technical meaning of the word culture.
- Culture is used in a special sense in anthropology and sociology. It refers to the sum of human beings’ lifeways, behavior, beliefs, feelings, and thoughts; it connotes everything acquired by them as social beings. Culture has been defined in several ways.
- There is no consensus among sociologists and anthropologists regarding the definition of culture.

Some Definitions of Culture

- According to British anthropologist Edward Taylor, “Culture is that complex whole which includes knowledge, belief, art, morals, law, custom and any other capabilities and habits acquired by man as a member of society”.
- According to Pathak, Bhagat, and Kashlak, “Culture is a concept that has been used in several social science disciplines to explain variations in human thought processes in different parts of the world.”
- According to J.P. Lederach, “Culture is the shared knowledge and schemes created by a set of people for perceiving, interpreting, expressing, and responding to the social realities around them.”

- According to R. Linton, “A culture is a configuration of learned behaviors and results of behavior whose component elements are shared and transmitted by the members of a particular society.”
- According to G. Hofstede, “Culture is the collective programming of the mind which distinguishes the members of one category of people from another.”
- According to H.T. Mazumdar, “Culture is the total of human achievements, material and non-material, capable of transmission, sociologically, i.e., by tradition and communication, vertically as well as horizontally.”
- Actually, culture is defined as the shared patterns of behaviors and interactions, cognitive constructs, and affective understanding that are learned through socialization. These shared patterns identify the members of a culture group while also distinguishing those of another group.

Internet?

- Internet as a communicational technology has opened a wide interdisciplinary field of research related with social and cultural change, a main topic in anthropological theory.
- The anthropological perspectives of culture implicit in different approaches to the analysis of Internet, specially those that refers to “cyberculture”, because this term contains a key concept of anthropological theory, and also it could be a good example for examining the use of anthropological theory for understanding media forms and practices, i.e., the Internet.

S Korea child starves as 'parents raise virtual baby'

A South Korean couple who were addicted to the internet let their three-month-old baby starve to death while raising a virtual daughter online, police said.

The pair fed their own premature baby just once a day in between 12-hour stretches at an internet cafe, the official Yonhap news agency reported.

Police officer Chung Jin-won told Yonhap they "lost their will to live a normal life" after losing their jobs.

He said they "indulged themselves online" to escape from reality.

The 41-year-old father and his 25-year-old wife were arrested in the city of Suweon, south of Seoul, earlier this week, five months after they reported the death of their baby.

An autopsy showed her death was caused by a long period of malnutrition.

The couple had become obsessed with nurturing a virtual girl called Anima in the popular role-playing game Prius Online, police said on Friday.

The game enables players to interact with Anima and as they do so, help her to recover her lost memory and develop emotions.

BBC News, March 5, 2010

Cyber-culture?

- What do we mean by “cyberculture”?
- People were using, and still use, the prefix “cyber” to refer to activities and social movements carried out through Internet, such as “cyberactivism”, “cybercafe”, “cyberart”, etc. It seems that the word “cyberculture” pretends to be a new concept to put together all these activities.
- It is seen that, “cyberculture” was used by some scholars as a concept for understanding the impact of internet on society.
- It is also seen that, “cyberculture” referred to a new interdisciplinary field of research, defined by the cultural analysis of communication and information technologies.

The map of Internet galaxy studies has four attractors:

a) Cyberculture as a new cultural model based on Internet technology

b) as an Internet emergent culture

c) as the cultural products developed in the Internet, and

d) as a media form.

These four elements are drawn down by using four main trends in conceptualizing culture: culture as an adaptive strategy, as a system whole, as a symbolic order and as signifying practice.

These different cultural perspectives also can be related with four major aspects in cyberculture studies:

a) Internet as a technology

b) Internet as a new social context

c) Internet as a new creative and collaborative tool

d) Internet as a medium of communication

- After the emergence of internet (21st century), Cyberculture was a topic of discussion in social sciences, most of them assuming that a new cultural model was emerging from Internet use that would change patterns of social relation, self identity and community.
- Some researchers also thought that Internet would bring a new way of political practice and economic exchange; thus, Internet was seen as a new technology that will affect all spheres of our life.
- Internet has been seen as a technology that will bring a new era which would lead to a new cultural order called Informational and Knowledge Society, Network Society –Manuel Castells- or Cyberculture –Pierre Lévy, Arturo Escobar.
- People, societies and states that will not participate in that technological revolution will be excluded of progress. Therefore, digital divide is seen as the new social definitive division, more important than other unequal divisions such as rich and poor, developed or undeveloped countries.

- Going further, technoculture, the imbrications (adjacent edges overlapping) of technology in human interactions and in human body itself, related with cognitive sciences, biotechnologies and genetics science, will change our conceptions of nature as opposed to culture, creating a new Anthropos or posthuman cyborg –Dona Haraway.
- David Hakken work Cyborgs @ Cyberspace, An Ethnographer looks to the Future is a useful contrasting point here, because he remembers us that these kind of theorizations need an empirical background and are strongly related with evolutionist and neo evolutionist theories in anthropology, and that there is an important field in anthropological work about technology innovation and culture change, such as Leslie White thesis, or recently, the social construction of technology theories of Bruno Latour and Wiebe Bijker, among others.

*Donna J. Haraway is an American Professor Emerita in the History of Consciousness Department and Feminist Studies Department at the University of California, Santa Cruz, United States. She is a prominent scholar in the field of science and technology studies, described in the early 1990s as a "feminist and postmodernist".

What is cybercrime?

- Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.
- Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.
- Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.
- Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

- Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.
- Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans.
- By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

- New technologies create new criminal opportunities but few new types of crime.
- **What distinguishes cybercrime from traditional criminal activity?**
- Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity.
- Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy.
- All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities.

- Most cybercrime is an attack on information about individuals, corporations, or governments.
- Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet.
- In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations.
- Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

- An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances.
- This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation.
- For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal?
- Where exactly does cybercrime take place?
- Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation.

- As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself.
- However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks.
- In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified.

- In 1996 the Council of Europe, together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime.
- Around the world, civil libertarian groups immediately protested provisions in the treaty requiring Internet service providers (ISPs) to store information on their customers' transactions and to turn this information over on demand.
- Work on the treaty proceeded nevertheless, and on November 23, 2001, the Council of Europe Convention on Cybercrime was signed by 30 states.
- The convention came into effect in 2004.

- Additional protocols, covering terrorist activities and racist and xenophobic cybercrimes, were proposed in 2002 and came into effect in 2006.
- In addition, various national laws, such as the USA PATRIOT Act of 2001, have expanded law enforcement's power to monitor and protect computer networks.

Types of cybercrime

- Cybercrime ranges across a spectrum of activities.
- At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual.
- Also at this end of the spectrum is the growing crime of identity theft.
- Midway along the spectrum lie transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting.
- These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the Internet.

- Another part of this type of crime involves individuals within corporations or government bureaucracies deliberately altering data for either profit or political objectives.

- At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet.

- These range from spam, hacking, and denial of service attacks against specific sites to acts of cyberterrorism—that is, the use of the Internet to cause public disturbances and even death.

- Cyberterrorism focuses upon the use of the Internet by nonstate actors to affect a nation's economic and technological infrastructure.

- Since the September 11 attacks of 2001, public awareness of the threat of cyberterrorism has grown dramatically.

Identity Theft and invasion of privacy

- **Identity theft**, also called **identity fraud**, use of an individual's personally identifying information by someone else (often a stranger) without that individual's permission or knowledge.
- This form of impersonation is often used to commit fraud, generally resulting in financial harm to the individual and financial gain to the impersonator.
- As the amount of personal information available on the Internet increased dramatically in the late 1990s and early 2000s, identity theft became a widespread concern.

- In the context of identity theft, identity refers to information intrinsic to a specific individual.
- Publicly available information, such as a person's telephone number and street address, as well as confidential information, such as (in the United States) a person's Social Security number, mother's maiden name, and credit card numbers, contribute to a person's identity.
- By acquiring access to that information, an identity thief can impersonate someone else to commit fraud.
- While identity theft is often associated with financial gain (i.e., the theft of money), it can also be used to acquire unauthorized entry, privileges, or benefits.

Methods

- Nonelectronic methods of identity theft include

  -stealing mail or rummaging through trash (“dumpster diving”)

  -eavesdropping on private conversations in public venues (“shoulder surfing”)

  - the theft of a wallet or purse.

- Personal records can be fraudulently obtained from government offices, and some thieves steal the identities of the deceased by using information collected from tombstones.

- Technology has added new dimensions to identity fraud.
- Small electronic devices called “skimmers” can be used to steal personal information from the magnetic strips on debit and credit cards.
- Skimmers allow thieves to copy cards for personal use and can be concealed under a counter, in an apron, or inside the card readers of gas station pumps or automated teller machines (ATMs).

- Similarly, the increasing amount of personally identifying information that is created, exchanged, stored, and maintained in computer databases creates new vulnerabilities.
- Personal computers provide a virtual playground for hackers, as a skillful thief can rifle through electronic data without authorization.
- Stolen information, which is often supplied through insider theft by company employees with access to records databases, can be bought and sold on illegal websites.
- New cybercrime techniques for facilitating identity fraud emerged as a result of society's growing use of and reliance on the Internet and e-mail.

- Phishing, for example, typically occurs when a fraudulent e-mail message (often spam) is used to direct a potential victim to a website that mimics the appearance of a familiar bank or e-commerce site.
- The person is then asked to “update” or “confirm” an account, thereby unwittingly disclosing confidential information.
- Domain name system (DNS) cache poisoning and pharming techniques employ fake websites that resemble those of legitimate businesses, tricking victims into unwittingly providing their personal information.
- Viruses, spyware, and malware can be used to track the activities of computer users and to gain access to the information on their hard drives, and hackers can “crack” security vulnerabilities in software programs to gain access to personal data via so-called Trojan horse applications.

- Although identity theft takes places in many countries, researchers and law-enforcement officials are plagued by a lack of information and statistics about the crime worldwide.
- Cybercrime is clearly, however, an international problem.
- In 2015 the U.S. Bureau of Justice Statistics (BJS) released a report on identity theft; in the previous year almost 1.1 million Americans had their identities fraudulently used to open bank, credit card, or utility accounts.
- The report also stated that another 16.4 million Americans were victimized by account theft, such as use of stolen credit cards and automatic teller machine (ATM) cards.

- The BJS report showed that while the total number of identity theft victims in the United States had grown by about 1 million since 2012, the total loss incurred by individuals had declined since 2012 by about $10 billion to $15.4 billion.
- Most of that decline was from a sharp drop in the number of people losing more than $2,000.
- Most identity theft involved small sums, with losses less than $300 accounting for 54 percent of the total.

Cyber Crime- scenario in India (Case study)

a) The Bank NSP Case

In this case, a management trainee of a bank got engaged through a marriage.

- The couple used to exchange many emails using the company's computers.
- After some time they had broken up their marriage and the young lady created some fake email ids such as "Indian bar associations" and sent mails to the boy's foreign clients.
- She used the banks computer to do this. The boy's company lost a huge number of clients and took the bank to court.
- The bank was held liable for the emails sent using the bank's system.

Bazee.com case

In December 2004 the Chief Executive Officer of Bazee.com was arrested because he was selling a compact disk (CD) with offensive material on the website, and even CD was also conjointly sold-out in the market of Delhi.

The Delhi police and therefore the Mumbai Police got into action and later the CEO was free on bail.

Parliament Attack Case

The Bureau of Police Research and Development, Hyderabad had handled this case.

A laptop was recovered from the terrorist who attacked the Parliament.

The laptop which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament was under siege, was sent to Computer Forensics Division of BPRD.

The laptop contained several proofs that affirmed the two terrorist's motives, mainly the sticker of the Ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal.

The emblems (of the 3 lions) were carefully scanned and additionally the seal was also craftly created together with a residential address of Jammu and Kashmir.

However careful detection proved that it was all forged and made on the laptop.

Andhra Pradesh Tax Case

The owner of the plastics firm in Andhra Pradesh was arrested and cash of Rs. 22 was recovered from his house by the Vigilance Department.

They wanted evidence from him concerning the unaccounted cash. The suspected person submitted 6,000 vouchers to prove the legitimacy of trade, however when careful scrutiny the vouchers and contents of his computers it unconcealed that every one of them were made after the raids were conducted.

It had been concealed that the suspect was running 5 businesses beneath the presence of 1 company and used fake and computerized vouchers to show sales records and save tax.

So the dubious techniques of the businessman from the state were exposed when officials of the department got hold of computers utilized by the suspected person.

SONY.SAMBANDH.COM CASE

India saw its 1st cybercrime conviction. This is the case where Sony India Private Limited filed a complaint that runs a website referred to as www.sony-sambandh.com targeting the NRIs.

The website allows NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the involved recipients.

In May 2002, somebody logged onto the web site underneath the identity of Barbara Campa and ordered a Sony colour television set and a cordless head phone. She requested to deliver the product to Arif Azim in Noida and gave the number of her credit card for payment.

The payment was accordingly cleared by the credit card agency and the transaction processed.

After the related procedures of dues diligence and checking, the items were delivered to Arif Azim by the company.

When the product was delivered, the company took digital pictures so as to indicate the delivery being accepted by Arif Azim.

The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company had filed a complaint for online cheating at the CBI that registered a case under the Section 418, Section 419 and Section 420 of the IPC (Indian Penal Code).

Arif Azim was arrested after the matter was investigated.

Investigations discovered that Arif Azim, whereas acting at a call Centre in Noida did gain access to the number of the credit card of an American national which he misused on the company's site.

The CBI recovered the color television along with the cordless head phone. In this matter, the CBI had proof to prove their case so the accused admitted his guilt.

The court had convicted Arif Azim under the Section 418, Section 419 and Section 420 of the IPC, this being the first time that a cybercrime has been convicted.

The court, felt that since the defendant was a boy of 24 years and a first time convict, a compassionate view needed to be taken.

Thus, the court discharged the defendant on the probation for one year. Section 67 and Section 70 of the IT Act are also applied. In this case the hackers hacks ones webpage and replace the homepage with pornographic or defamatory page.

Cyber Laws in India

Following are the sections under IT Act, 2000

1. Section 65-

Tampering with the computers source documents

Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for a computer, computer program, and computer system or computer network.

Punishment: Any person who involves in such crimes could be sentenced upto 3 years imprisonment or with a fine of Rs.2 lakhs or with both.

Section 66-

Hacking with computer system, data alteration etc. Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer.

Diminish its utility, values or affects it injuriously by any means, commits hacking.

Punishment: Any person who involves in such crimes could be sentenced upto 3 years imprisonment, or with a fine that may extend upto 2 lakhs rupees, or both

Section 66A- Sending offensive messages through any communication services

Any information or message sent through any communication services this is offensive or has threatening characters.

Any information that is not true or is not valid and is sent with the end goal of annoying, inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred or ill will.

Any electronic mail or email sent with the end goal of causing anger, difficulty or mislead or to deceive the address about the origin of the messages.

Punishment: Any individual found to commit such crimes under this section could be sentenced upto 3 years of imprisonment along with a fine

Section 66B- Receiving stolen computer's resources or communication devices dishonestly

Receiving or retaining any stolen computer, computer's resources or any communication devices knowingly or having the reason to believe the same.

Punishment: Any person who involves in such crimes could be sentenced either description for a term that may extend upto 3 years of imprisonment or with a fine of rupee 1 lakh or both.

Section 66C- Identify theft

Using of one's digital or electronic signature or one's password or any other unique identification of any person is a crime.

Punishment: Any person who involve in such crimes could be sentenced either with a description for a term which may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

Section 66D- Cheating by personation by the use of computer's resources

Whoever tries to cheats someone by personating through any communication devices or computer's resources shall be sentenced either with a description for a term that may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

Section 66E- Privacy or violation

Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas or private parts of any individual without his/her consent, that violates the privacy of the individual shall be sentenced to 3 years of imprisonment or with a fine not exceeding more than 2 lakhs rupees or both.

Section 66F- Cyber terrorism

A. Whoever intentionally threatened the integrity, unity, sovereignty or security or strike terror among the people or among any group of people by

I. Deny to any people to access computer's resources.

II. Attempting to break in or access a computer resource without any authorization or to exceed authorized access.

III. Introducing any computer's contaminant, and through such conducts causes or is probable to cause any death or injury to any individual or damage or any destruction of properties or disrupt or it is known that by such conduct it is probable to cause damage or disruptions of supply or services that are essential to the life of people or unfavorably affect the critical information's infrastructure specified under the section 70 of the IT Act.

B. By intention or by knowingly tries to go through or tries to gain access to computer's resources without the authorization or exceeding authorized access, and by such conducts obtains access to the data, information or computer's database which is limited or restricted for certain reason because of the security of the state or foreign relations, or any restricted database, data or any information with the reason to believe that those data or information or the computer's database obtained may use to cause or probably use to cause injury to the interest of the independence and integrity of our country India.

Punishment: Whoever conspires or commits such cyber crime or cyber terrorism shall be sentenced to life time imprisonment.

Section 67- Transmitting or publishing obscene materials in electronic form

Whoever transmits or publishes or cause to publish any obscene materials in electronics form. Any material that is vulgar or appeal to be lubricious or if its effect is for instance to tends to corrupt any individual who are likely to have regard to all relevant circumstances to read or to see or to hear the matter that contained in it, shall be sentenced on the first convict with either description for a term that may extend upto five years of imprisonment along with a fine which may extend upto 1 lakh rupee and in the second or subsequent convict it can be sentenced either description for a term that may extend upto ten years along with a fine that may perhaps extend to two lakhs rupees.

Section 67A- Transmitting or publishing of materials that contains sexually explicit contents, acts etc in electronics form

Whoever transmits or publishes materials that contains sexually explicit contents or acts shall be sentences for either description for a term which may extend upto 5 years or imprisonment along with a fine that could extend to 10 lakhs rupees in the first convict. And in the event of the second convict criminal could be sentenced for either description for a term that could extend upto 7 years of imprisonment along with a fine that may extend upto 20 lakhs rupees.

Section 67B- Transmitting or publishing of materials that depicts children in sexually explicit act etc. in electronics form

Whoever transmits or publishes any materials that depict children in sexually explicit act or conduct in any electronics form shall be sentenced for either description for a term which may extend to 5 years of imprisonment with a fine that could extend to rupees 10 lakhs on the first conviction. And in the event of second conviction criminals could be sentenced for either description for a term that could extend to 7 years along with a fine that could extend to rupees 10 lakhs.

Section 67C- Retention and preservation of information by intermediaries

I. Intermediaries shall retain and preserve such information that might specify for such period and in such a format and manner that the Central Government may prescribe.

II. Any intermediaries knowingly or intentionally contravene the provision of the sub-section.

Punishment: Whoever commits such crimes shall be sentenced for a period that may extend upto 3 years of imprisonment and also liable to fine

Section 69- Power to issue direction for monitor, decryption or interception of any information through computer's resources

I. Where the Central government's or State government's authorized officers, as the case may be in this behalf, if fulfilled that it is required or expedient to do in the interest of the integrity or the sovereignty, the security defence of our country India, state's security, friendly relations with the foreign states for preventing any incident to the commission of any cognizable offences that is related to above or investigation of any offences that is subjected to the provision of sub-section

(II). For reasons to be recorded writing, direct any agency of the appropriate government, by order, decrypt or monitor or cause to be intercept any information that is generated or received or transmitted or is stored in any computer's resources.

II. The safeguard and the procedure that is subjected to such decryption, monitoring or interception may carried out, shall be such as may be prescribed.

III. The intermediaries, the subscribers or any individual who is in the charge of the computer's resources shall call upon by any agencies referred to the sub-section (I), extends all services and technical assistances to:

a) Providing safe access or access to computer's resources receiving, transmitting, generating or to store such information or b) Decrypting, intercepting or monitoring the information, as the case might be or c) Providing information that is stored in computer.

IV. The intermediaries, the subscribes or any individual who fails to help the agency referred in the sub-section (III), shall be sentenced for a term that could extend to 7 years of imprisonment and also could be legally responsible to fine [17].

Internet Fraud

Schemes to defraud consumers abound on the Internet. Among the most famous is the Nigerian, or “419,” scam; the number is a reference to the section of Nigerian law that the scam violates.

Although this con has been used with both fax and traditional mail, it has been given new life by the Internet.

In the scheme, an individual receives an e-mail asserting that the sender requires help in transferring a large sum of money out of Nigeria or another distant country.

Usually, this money is in the form of an asset that is going to be sold, such as oil, or a large amount of cash that requires “laundering” to conceal its source; the variations are endless, and new specifics are constantly being developed.

The message asks the recipient to cover some cost of moving the funds out of the country in return for receiving a much larger sum of money in the near future.

Should the recipient respond with a check or money order, he is told that complications have developed; more money is required. Over time, victims can lose thousands of dollars that are utterly unrecoverable.

- In 2002 the newly formed U.S. Internet Crime Complaint Center (IC3) reported that more than $54 million dollars had been lost through a variety of fraud schemes; this represented a threefold increase over estimated losses of $17 million in 2001.
- The annual losses grew in subsequent years, reaching $125 million in 2003, about $200 million in 2006, close to $250 million in 2008, and over $1 billion in 2015.
- In the United States the largest source of fraud is what IC3 calls “non-payment/non-delivery,” in which goods and services either are delivered but not paid for or are paid for but not delivered.

- Despite a vast amount of consumer education, Internet fraud remains a growth industry for criminals and prosecutors.
- Europe and the United States are far from the only sites of cybercrime.
- South Korea is among the most wired countries in the world, and its cybercrime fraud statistics are growing at an alarming rate. Japan has also experienced a rapid growth in similar crimes.

ATM Fraud

- Computers also make more mundane types of fraud possible.
- Take the automated teller machine (ATM) through which many people now get cash.
- In order to access an account, a user supplies a card and personal identification number (PIN).
- Criminals have developed means to intercept both the data on the card's magnetic strip as well as the user's PIN.
- In turn, the information is used to create fake cards that are then used to withdraw funds from the unsuspecting individual's account.
- For example, in 2002 the *New York Times* reported that more than 21,000 American bank accounts had been skimmed by a single group engaged in acquiring ATM information illegally.

- A particularly effective form of fraud has involved the use of ATMs in shopping centres and convenience stores.
- These machines are free-standing and not physically part of a bank.
- Criminals can easily set up a machine that looks like a legitimate machine; instead of dispensing money, however, the machine gathers information on users and only tells them that the machine is out of order after they have typed in their PINs.
- Given that ATMs are the preferred method for dispensing currency all over the world, ATM fraud has become an international problem.

Wire fraud

- The international nature of cybercrime is particularly evident with wire fraud.
- One of the largest and best-organized wire fraud schemes was orchestrated by Vladimir Levin, a Russian programmer with a computer software firm in St. Petersburg.
- In 1994, with the aid of dozens of confederates, Levin began transferring some $10 million from subsidiaries of Citibank, N.A., in Argentina and Indonesia to bank accounts in San Francisco, Tel Aviv, Amsterdam, Germany, and Finland.
- According to Citibank, all but $400,000 was eventually recovered as Levin's accomplices attempted to withdraw the funds.
- Levin himself was arrested in 1995 while in transit through London's Heathrow Airport (at the time, Russia had no extradition treaty for cybercrime).

- In 1998 Levin was finally extradited to the United States, where he was sentenced to three years in jail and ordered to reimburse Citibank $240,015.
- Exactly how Levin obtained the necessary account names and passwords has never been disclosed, but no Citibank employee has ever been charged in connection with the case.
- Because a sense of security and privacy are paramount to financial institutions, the exact extent of wire fraud is difficult to ascertain.
- In the early 21st century, wire fraud remained a worldwide problem.

File Sharing and Piracy

- Through the 1990s, sales of compact discs (CDs) were the major source of revenue for recording companies.
- Although piracy—that is, the illegal duplication of copyrighted materials—had always been a problem, especially in the Far East, the proliferation on college campuses of inexpensive personal computers capable of capturing music off CDs and sharing them over high-speed ("broadband") Internet connections became the recording industry's greatest nightmare.
- In the United States, the recording industry, represented by the Recording Industry Association of America (RIAA), attacked a single file-sharing service, Napster, which from 1999 to 2001 allowed users across the Internet access to music files, stored in the data-compression format known as MP3, on other users' computers by way of Napster's central computer.

- According to the RIAA, Napster users regularly violated the copyright of recording artists, and the service had to stop.
- For users, the issues were not so clear-cut. At the core of the Napster case was the issue of fair use.
- Individuals who had purchased a CD were clearly allowed to listen to the music, whether in their home stereo, automobile sound system, or personal computer.
- What they did not have the right to do, argued the RIAA, was to make the CD available to thousands of others who could make a perfect digital copy of the music and create their own CDs.

- Users rejoined that sharing their files was a fair use of copyrighted material for which they had paid a fair price.
- In the end, the RIAA argued that a whole new class of cybercriminal had been born—the digital pirate—that included just about anyone who had ever shared or downloaded an MP3 file.
- Although the RIAA successfully shuttered Napster, a new type of file-sharing service, known as peer-to-peer (P2P) networks, sprang up.
- These decentralized systems do not rely on a central facilitating computer; instead, they consist of millions of users who voluntarily open their own computers to others for file sharing.
- The RIAA continued to battle these file-sharing networks, demanding that ISPs turn over records of their customers who move large quantities of data over their networks, but the effects were minimal.

- The RIAA's other tactic has been to push for the development of technologies to enforce the digital rights of copyright holders.
- So-called digital rights management (DRM) technology is an attempt to forestall piracy through technologies that will not allow consumers to share files or possess "too many" copies of a copyrighted work.
- At the start of the 21st century, copyright owners began accommodating themselves with the idea of commercial digital distribution.
- Examples include the online sales by the iTunes Store (run by Apple Inc.) and Amazon.com of music, television shows, and movies in downloadable formats, with and without DRM restrictions.
- In addition, several cable and satellite television providers, many electronic game systems (Sony Corporation's PlayStation 3 and Microsoft Corporation's Xbox 360), and streaming services like Netflix developed "video-on-demand" services that allow customers to download movies and shows for immediate (streaming) or later playback.

- File sharing brought about a fundamental reconstruction of the relationship between producers, distributors, and consumers of artistic material.
- In America, CD sales dropped from a high of nearly 800 million albums in 2000 to less than 150 million albums in 2014. Although the music industry sold more albums digitally than it had CDs at its peak, revenue declined by more than half since 2000.
- As broadband Internet connections proliferate, the motion-picture industry faces a similar problem, although the digital videodisc (DVD) came to market with encryption and various built-in attempts to avoid the problems of a video Napster.
- However, sites such as The Pirate Bay emerged that specialized in sharing such large files as those of movies and electronic games.

Counterfeiting and Forgery

- The advent of inexpensive, high-quality colour copiers and printers has brought counterfeiting to the masses.
- Ink-jet printers now account for a growing percentage of the counterfeit currency confiscated by the U.S. Secret Service.
- In 1995 ink-jet currency accounted for 0.5 percent of counterfeit U.S. currency; in 1997 ink-jet printers produced 19 percent of the illegal cash.
- By 2014 almost 60 percent of the counterfeit money recovered in the U.S. came from ink-jet printers.
- The widespread development and use of computer technology prompted the U.S. Treasury to redesign U.S. paper currency to include a variety of anticounterfeiting technologies.
- The European Union currency, or euro, had security designed into it from the start. Special features, such as embossed foil holograms and special ribbons and paper, were designed to make counterfeiting difficult.

- Currency is not the only document being copied. Immigration documents are among the most valuable, and they are much easier to duplicate than currency.
- In the wake of the September 11 attacks, this problem came under increasing scrutiny in the United States.
- In particular, the U.S. General Accounting Office (GAO) issued several reports during the late 1990s and early 2000s concerning the extent of document fraud that had been missed by the Immigration and Naturalization Service (INS).
- Finally, a 2002 report by the GAO reported that more than 90 percent of certain types of benefit claims were fraudulent and further stated that immigration fraud was “out of control.”
- Partially in response to these revelations, the INS was disbanded and its functions assumed by the newly constituted U.S. Department of Homeland Security in 2003.

Child Pornography

- With the advent of almost every new media technology, pornography has been its "killer app," or the application that drove early deployment of technical innovations in search of profit.
- The Internet was no exception, but there is a criminal element to this business bonanza—child pornography, which is unrelated to the lucrative business of legal adult-oriented pornography.
- The possession of child pornography, which generally are images of children under age 18 engaged in sexual behaviour, is illegal in the United States, the European Union, and many other countries, but it remains a problem that has no easy solution.

- The problem is compounded by the ability of “kiddie porn” websites to disseminate their material from locations, such as states of the former Soviet Union as well as Southeast Asia, that lack cybercrime laws.
- Some law-enforcement organizations believe that child pornography represents a $3-billion-a-year industry and that more than 10,000 Internet locations provide access to these materials.
- The Internet also provides pedophiles with an unprecedented opportunity to commit criminal acts through the use of “chat rooms” to identify and lure victims.

- Here the virtual and the material worlds intersect in a particularly dangerous fashion.
- In many countries, state authorities now pose as children in chat rooms; despite the widespread knowledge of this practice, pedophiles continue to make contact with these "children" in order to meet them "off-line."
- That such a meeting invites a high risk of immediate arrest does not seem to deter pedophiles.
- Interestingly enough, it is because the Internet allows individual privacy to be breached that the authorities are able to capture pedophiles.

Indian Perspective

- The government said that the Supreme Court of India in two judgements had directed it to frame necessary guidelines to eliminate child pornography and related contents in online platforms and other applications.
- And in the second case, the court had said that it was imperative to frame proper regime to find out the persons, institutions, and bodies who were the originators of such content messages.
- The Indian Parliament (Upper House - Rajya Sabha) had repeatedly asked the Govt. of India to strengthen the legal framework and make the social media platforms accountable under the Indian laws.

- Commenting on concerns around traceability of the first originator of the information, the government said that that the new IT rules seeks only limited information and only when a message already in public circulation is giving rise to violence, impinging on the unity and integrity of India, depicting a woman in a bad light, or sexual abuse of a child.
- When no other intrusive options are working, only then the significant social media intermediary will be required to disclose as to who started the message.
- It said that the concern that the rules may be misused deliberately to make a large number of complaints so as to overwhelm the grievance redressal mechanisms created by social media platforms is also misplaced, exaggerated and disingenuous and shows lack of willingness to address the grievances of the users of these media platforms while using their data to earn revenues.

- The government of India fully recognises and respects the right of privacy, as pronounced by the Supreme Court of India in KS Puttusamy case.
- Privacy is the core element of an individual's existence and, in light of this, the new IT rules seeks information only on a message that is already in circulation that resulted in an offence. The rules have framed in exercise of the statutory powers of the IT Act, fully taking into account the principles of reasonableness and proportionality.
- Twitter has written to the government that it intends to comply with the new IT rules but has not been able to do so due to the Covid pandemic.
- Facebook, WhatsApp, YouTube etc. have complied with the new rules but WhatsApp has challenged the guidelines before court.
- Twitter has also been pulled up by a Parliamentary committee headed by Lok Sabha member Shashi Tharoor for failing to comply with Indian rules.

Justice K. S. Puttaswamy v. Union of India-The Supreme Court held that a fundamental right to privacy is guaranteed under the Constitution of India. On 23rd August 2017, the Supreme Court unanimously recognised privacy as a fundamental right guaranteed by the Constitution.

BACKGROUND OF THE CASE:

This case was brought by 91 year old retired High Court Judge Puttaswamy against the Union of India before a nine- judge's bench to determine whether the **Right to Privacy** was guaranteed as an independent Fundamental Right.

On the 24th of August 2017, a nine judge's bench of the Supreme Court delivered its verdict in Justice ***K.S.Puttaswamy (Retd.) v. Union of India & Others.***, unanimously affirming that "the Right to Privacy is a fundamental right under Article 21 of the Indian Constitution, which states that, no person shall be deprived of his right to life and personal liberty except according to the procedure established by law".

This case also challenged government's Aadhaar scheme (a uniform biometric based identity card), which was made necessary to access government services and benefits.

This case also overruled the decision made in the case of:

- **P. Sharma v. Satish Chandra**, and,
- **Kharak Singh v. State of Uttar Pradesh**, wherein both the cases, it was held that right to privacy is not a fundamental right.

Thus a nine judge's bench was set up to determine, whether right to privacy is a fundamental right under the Indian Constitution or not? The bench of Supreme Court unanimously gave its verdict that the Constitution guaranteed the right to privacy as an intrinsic part of Right to Life and Personal Liberty and the verdict ended the constitutional battle that had begun almost exactly two years ago.

Hacking

- While breaching privacy to detect cybercrime works well when the crimes involve the theft and misuse of information, ranging from credit card numbers and personal data to file sharing of various commodities—music, video, or child pornography—what of crimes that attempt to wreak havoc on the very workings of the machines that make up the network?
- The story of hacking actually goes back to the 1950s, when a group of phreaks (short for "phone freaks") began to hijack portions of the world's telephone networks, making unauthorized long-distance calls and setting up special "party lines" for fellow phreaks.
- With the proliferation of computer bulletin board systems (BBSs) in the late 1970s, the informal phreaking culture began to coalesce into quasi-organized groups of individuals who graduated from the telephone network to "hacking" corporate and government computer network systems.

- Although the term *hacker* predates computers and was used as early as the mid-1950s in connection with electronic hobbyists, the first recorded instance of its use in connection with computer programmers who were adept at writing, or "hacking," computer code seems to have been in a 1963 article in a student newspaper at the Massachusetts Institute of Technology (MIT).
- After the first computer systems were linked to multiple users through telephone lines in the early 1960s, *hacker* came to refer to individuals who gained unauthorized access to computer networks, whether from another computer network or, as personal computers became available, from their own computer systems.
- It is interesting to know about the hacker culture, most hackers have not been criminals in the sense of being vandals or of seeking illicit financial rewards.

- Instead, most have been young people driven by intellectual curiosity; many of these people have gone on to become computer security architects.
- However, as some hackers sought notoriety among their peers, their exploits led to clear-cut crimes.
- In particular, hackers began breaking into computer systems and then bragging to one another about their exploits, sharing pilfered documents as trophies to prove their boasts.
- These exploits grew as hackers not only broke into but sometimes took control of government and corporate computer networks.

- One such criminal was Kevin Mitnick, the first hacker to make the “most wanted list” of the U.S. Federal Bureau of Investigation (FBI).
- He allegedly broke into the North American Aerospace Defense Command (NORAD) computer in 1981, when he was 17 years old, a feat that brought to the fore the gravity of the threat posed by such security breaches.
- Concern with hacking contributed first to an overhaul of federal sentencing in the United States, with the 1984 Comprehensive Crime Control Act and then with the Computer Fraud and Abuse Act of 1986.

- The scale of hacking crimes is among the most difficult to assess because the victims often prefer not to report the crimes—sometimes out of embarrassment or fear of further security breaches.
- Officials estimate, however, that hacking costs the world economy billions of dollars annually.
- Hacking is not always an outside job—a related criminal endeavour involves individuals within corporations or government bureaucracies deliberately altering database records for either profit or political objectives.
- The greatest losses stem from the theft of proprietary information, sometimes followed up by the extortion of money from the original owner for the data's return.
- In this sense, hacking is old-fashioned industrial espionage by other means.

- One of the largest known case of computer hacking was discovered in late March 2009.
- It involved government and private computers in at least 103 countries.
- The worldwide spy network known as GhostNet was discovered by researchers at the University of Toronto, who had been asked by representatives of the Dalai Lama to investigate the exiled Tibetan leader's computers for possible malware.
- In addition to finding out that the Dalai Lama's computers were compromised, the researchers discovered that GhostNet had infiltrated more than a thousand computers around the world.

- The highest concentration of compromised systems were within embassies and foreign affairs bureaus of or located in South Asian and Southeast Asian countries
- Reportedly, the computers were infected by users who opened e-mail attachments or clicked on Web page links.
- Once infected with the GhostNet malware, the computers began “phishing” for files throughout the local network—even turning on cameras and video-recording devices for remote monitoring.
- Three control servers that ran the malware were located in Hainan, Guangdong, and Sichuan provinces in China, and a fourth server was located in California.

Hacking in India

- Politicians, companies and activists are increasingly being targeted by a secretive industry. How does it work?
- What really blew the lid on this phenomenon was an exposé by the Canadian internet security watchdog, Citizen Lab, which outed a Delhi-based firm called Belltrox Infotech (2020).

How India became a hack-for-hire hub?

One evening in January, a Kanpur-based college student in his early 20s got a phone call from an unknown number. The engineering undergraduate, who did not wish to be identified, had been spending a lot of time on dark web forums. He'd even been searching for "hacking tutorials" on Google. His digital footprint had left behind a trail.

The caller surprisingly knew all about it. The offer was simple: Since you are interested in hacking, do you want to earn some money by hacking companies? It was a recruitment call. And the phone number, while difficult to trace, seemed to be from Florida.

Around the same time, the Kanpur-based hacker’s friend got a call too—because he had an adequate amount of “cred" on the dark web, he said. It was a more specific request: Steal the partner list of home services startup Urban Company (formerly UrbanClap). These lists contain the names and details of service personnel like barbers, repairmen, etc., who are employed by the company to perform jobs via its platforms. The “client" was willing to pay ₹40,000 in bitcoin for the data.

The second hacker refused to take up the offer, but said people like him often get such requests and they don’t even necessarily come via the dark web. Requests sometimes come via WhatsApp, through friends in the security community, or even through encrypted email services like Proton Mail.

It is a peek into the underbelly of an industry which is often described using a broad umbrella term: hack for hire. The targets are varied: corporate employees, politicians, and even ex-lovers sometimes. And what’s on offer is often “low-level" hacking—email passwords, access to social media accounts. With very few avenues to make money as an ethical hacker in India, talented young engineers or upstarts who wish to experiment have been exploring the dark side for a while now. And their numbers are increasing.

A May 2020 Google Threat Analysis Group (TAG) report highlighted an interesting emerging trend: that these “hack for hire" operations are now increasingly being mounted under the aegis of formally registered firms. “Many are based in India," the report said.

What really blew the lid on this new phenomenon, however, was an exposé by the Canadian internet security watchdog, Citizen Lab, which outed an obscure Delhi-based company called Belltrox Infotech Services Pvt. Ltd. First reported by Reuters, Citizen Lab's investigation reveals a sustained years-long hack for hire operation which targeted senior elected officials, businesses and even journalists, many of them based in jurisdictions outside India.

Security researchers had been trying to pin down the group of hackers operating under the shadow of Belltrox for years. The earliest identified victim goes back to 2017. Before the Delhi-based firm was identified, security researchers even had code words to describe what seemed to be eerily similar hacking attempts: Dark Basin hackers, mercenary armada.

According to three hackers (including the Delhi-based hacker mentioned earlier) who spoke to the concerned people (Mint) on the condition of anonymity, building this kind of business **hack for hire services (HaaS)** requires persistence. The “hustle" starts with “building a rep" on dark web forums; then finding clients; and then persisting till a target is compromised. If one wants foreign clients, building cred is vital. Black hats (those who hack into a computer network with malicious intent) choose to do this on the dark web, or by hiding their tracks in broad daylight.

The primary requirement for the hustle is a sustained presence on forums in the dark or deep web. The deep web refers to websites that aren’t indexed by search engines like Google, while the dark web is the same but can only be accessed through an anonymizing browser like Tor.

India adds a layer of its own to this industry. Jobs come through WhatsApp messages, Telegram, and more. And often, from just regular people or budding startups looking to topple highly-funded competitors. “My request was through someone in IT security. The target was a high-ranking official. The request was to gather information, gain entry into their Facebook and other social media accounts," said an Indian cyber forensic expert who had also been approached for hack for hire services.

The Indian cyber forensics expert told journalists that the real-estate sector often uses HaaS for their work. “I got information about a hack two years ago, and the modus operandi revealed confidential information of senior political party members, real estate targets, and more," he said. “Hackers start off with a phishing attack. If the target isn’t compromised, they change course and go for the nearest connection to the target. The aim is to get confidential information and get an edge," he added.

According to XYZ (details not to be revealed), many freelancers and part-time hackers from India make money from HaaS businesses. The managing director of a private detective agency told this news agency that his company receives approximately 150-200 queries per month from people who have had their email accounts, Facebook, etc., hacked.

The firm handles a lot of blackmailing cases in the country, and he said there are two kinds of blackmailers—those in which someone is being blackmailed directly and others where someone has obtained information about a person by hacking an email ID.

Computer Viruses

- The deliberate release of damaging computer viruses is yet another type of cybercrime.
- In fact, this was the crime of choice of the first person to be convicted in the United States under the Computer Fraud and Abuse Act of 1986.
- On November 2, 1988, a computer science student at Cornell University named Robert Morris released a software "worm" onto the Internet from MIT (as a guest on the campus, he hoped to remain anonymous).
- The worm was an experimental self-propagating and replicating computer program that took advantage of flaws in certain e-mail protocols.
- Due to a mistake in its programming, rather than just sending copies of itself to other computers, this software kept replicating itself on each infected system, filling all the available computer memory.
- Before a fix was found, the worm had brought some 6,000 computers (one-tenth of the Internet) to a halt.

- Although Morris's worm cost time and millions of dollars to fix, the event had few commercial consequences, for the Internet had not yet become a fixture of economic affairs.
- That Morris's father was the head of computer security for the U.S. National Security Agency led the press to treat the event more as a high-tech Oedipal drama than as a foreshadowing of things to come.
- Since then, ever more harmful viruses have been cooked up by anarchists and misfits from locations as diverse as the United States, Bulgaria, Pakistan, and the Philippines.

Denial of Service Attacks

- One can compare the Morris worm with the events of the week of February 7, 2000, when "mafiaboy," a 15-year-old Canadian hacker, orchestrated a series of denial of service attacks (DoS) against several e-commerce sites, including Amazon.com and eBay.com.
- These attacks used computers at multiple locations to overwhelm the vendors' computers and shut down their World Wide Web (WWW) sites to legitimate commercial traffic.
- The attacks crippled Internet commerce, with the FBI estimating that the affected sites suffered $1.7 billion in damages.
- In 1988 the Internet played a role only in the lives of researchers and academics; by 2000 it had become essential to the workings of the U.S. government and economy.

- Cybercrime had moved from being an issue of individual wrongdoing to being a matter of national security.
- Distributed DoS attacks are a special kind of hacking.
- A criminal salts an array of computers with computer programs that can be triggered by an external computer user.
- These programs are known as Trojan horses since they enter the unknowing users' computers as something benign, such as a photo or document attached to an e-mail.
- At a predesignated time, this Trojan horse program begins to send messages to a predetermined site.
- If enough computers have been compromised, it is likely that the selected site can be tied up so effectively that little if any legitimate traffic can reach it.

- One important insight offered by these events has been that much software is insecure, making it easy for even an unskilled hacker to compromise a vast number of machines.
- Although software companies regularly offer patches to fix software vulnerabilities, not all users implement the updates, and their computers remain vulnerable to criminals wanting to launch DoS attacks.
- In 2003 the Internet service provider PSINet Europe connected an unprotected server to the Internet.
- Within 24 hours the server had been attacked 467 times, and after three weeks more than 600 attacks had been recorded.
- Only vigorous security regimes can protect against such an environment. Despite the claims about the pacific nature of the Internet, it is best to think of it as a modern example of the Wild West of American lore—with the sheriff far away.

Spam, steganography, and e-mail hacking

- E-mail has spawned one of the most significant forms of cybercrime—spam, or unsolicited advertisements for products and services, which experts estimate to comprise roughly 50 percent of the e-mail circulating on the Internet.
- Spam is a crime against all users of the Internet since it wastes both the storage and network capacities of ISPs, as well as often simply being offensive.
- Yet, despite various attempts to legislate it out of existence, it remains unclear how spam can be eliminated without violating the freedom of speech in a liberal democratic polity.
- Unlike junk mail, which has a postage cost associated with it, spam is nearly free for perpetrators—it typically costs the same to send 10 messages as it does to send 10 million.

- One of the most significant problems in shutting down spammers involves their use of other individuals' personal computers.
- Typically, numerous machines connected to the Internet are first infected with a virus or Trojan horse that gives the spammer secret control.
- Such machines are known as zombie computers, and networks of them, often involving thousands of infected computers, can be activated to flood the Internet with spam or to institute DoS attacks.
- While the former may be almost benign, including solicitations to purchase legitimate goods, DoS attacks have been deployed in efforts to blackmail Web sites by threatening to shut them down.
- Cyber experts estimate that the United States accounts for about one-fourth of the 4–8 million zombie computers in the world and is the origin of nearly one-third of all spam.

- E-mail also serves as an instrument for both traditional criminals and terrorists.
- While libertarians laud the use of cryptography to ensure privacy in communications, criminals and terrorists may also use cryptographic means to conceal their plans.
- Law-enforcement officials report that some terrorist groups embed instructions and information in images via a process known as steganography, a sophisticated method of hiding information in plain sight.
- Even recognizing that something is concealed in this fashion often requires considerable amounts of computing power; actually decoding the information is nearly impossible if one does not have the key to separate the hidden data.

- In a type of scam called business e-mail compromise (BEC), an e-mail sent to a business appears to be from an executive at another company with which the business is working.
- In the e-mail, the "executive" asks for money to be transferred into a certain account. The FBI has estimated that BEC scams have cost American businesses about $750 million.
- Sometimes e-mail that an organization would wish to keep secret is obtained and released. In 2014 hackers calling themselves "Guardians of Peace" released e-mail from executives at the motion picture company Sony Pictures Entertainment, as well as other confidential company information.
- The hackers demanded that Sony Pictures not release *The Interview*, a comedy about a CIA plot to assassinate North Korean leader Kim Jong-Un, and threatened to attack theatres that showed the movie.

- After American movie theatre chains canceled screenings, Sony released the movie online and in limited theatrical release.
- E-mail hacking has even affected politics. In 2016, e-mail at the Democratic National Committee (DNC) was obtained by hackers believed to be in Russia.
- Just before the Democratic National Convention, the media organization WikiLeaks released the e-mail, which showed a marked preference of DNC officials for the presidential campaign of Hillary Clinton over that of her challenger Bernie Sanders.
- DNC chairperson Debbie Wasserman Schultz resigned, and some American commentators speculated that the release of the e-mail showed the preference of the Russian government for Republican nominee Donald Trump.

Sabotage

- Another type of hacking involves the hijacking of a government or corporation Website.
- Sometimes these crimes have been committed in protest over the incarceration of other hackers; in 1996 the Web site of the U.S. Central Intelligence Agency (CIA) was altered by Swedish hackers to gain international support for their protest of the Swedish government's prosecution of local hackers, and in 1998 the *New York Times*'s Web site was hacked by supporters of the incarcerated hacker Kevin Mitnick.
- Still other hackers have used their skills to engage in political protests: in 1998 a group calling itself the Legion of the Underground declared "cyberwar" on China and Iraq in protest of alleged human rights abuses and a program to build weapons of mass destruction, respectively.

- In 2007, Estonian government Web sites, as well as those for banks and the media, were attacked.
- Russian hackers were suspected because Estonia was then in a dispute with Russia over the removal of a Soviet war memorial in Tallinn.
- Sometimes a user's or organization's computer system is attacked and encrypted until a ransom is paid. The software used in such attacks has been dubbed *ransomware*.
- The ransom usually demanded is payment in a form of virtual currency, such as Bitcoin. When data are of vital importance to an organization, sometimes the ransom is paid.
- In 2016 several American hospitals were hit with ransomware attacks, and one hospital paid over $17,000 for its systems to be released.

- Defacing Web sites is a minor matter, though, when compared with the specter of cyberterrorists using the Internet to attack the infrastructure of a nation, by rerouting airline traffic, contaminating the water supply, or disabling nuclear plant safeguards.
- One consequence of the September 11 attacks on New York City was the destruction of a major telephone and Internet switching centre.
- Lower Manhattan was effectively cut off from the rest of the world, save for radios and cellular telephones. Since that day, there has been no other attempt to destroy the infrastructure that produces what has been called that “consensual hallucination,” cyberspace.
- Large-scale cyberwar (or “information warfare”) has yet to take place, whether initiated by rogue states or terrorist organizations, although both writers and policy makers have imagined it in all too great detail.

Attacks in the history of cyber crimes that shook the entire world!

Yahoo Data Breach

- The Yahoo data breach broke all records of data theft in the history of cyber crimes.
- Yahoo found itself at the target point of hackers not once but twice as it came to terms with more than 3 billion user accounts being stolen!
- This incident put personal information such as name, phone number, email ID and passwords of 3 billion users out in the open!
- And the mystery continues till date as Yahoo struggles to find how this data breach was initiated and executed.

Ransomware WannaCry

- Midway through 2017, the United Kingdom fell prey to one of the most devious cyber attacks it had ever faced – ransomware WannaCry.
- Delivered as an email attachment virus, it locked up all files in an MS Windows powered system, eventually demanding a ransom for unlocking them.
- Having started as an attack on their NHS computer system, the ransomware had slowly brought systems from the UK to the US and from Russia to China to their knees.
- As many as 300,000 computers over 150 countries were infected by WannaCry.

The Logic Bomb

- Considered as one of the most devastating attacks in the history of cyber crimes, the aftermath of this logic bomb was way beyond a monetary tally.
- It involved the Americans embedding a piece of code to the Russians during the cold war of 1982.
- Once this code which was used to control a pipeline for transporting natural gas from Siberia was activated, it caused an explosion so strong that it could be seen even through space!

Sony Pictures

- In 2011, Sony's data storage was hacked exposing the records of over 100 million customers using their PlayStation's online services.
- What was shocking was that the hackers had access to all the credit card information of users apart from personal details!
- This data breach cost Sony over 171 million USD.

Petya / NotPetya / Nyetya / Goldeneye

- The world had barely recovered from the impact of WannaCry when another wave of ransomware infections was unleashed onto networks all around the globe.
- Called Petya, NotPetya and by a few other names, it hit networks across multiple countries, the notables ones being the US pharmaceutical company Merck, Danish shipping company Maersk, and Russian oil giant Rosneft.
- Research has revealed that this ransomware attack was actually intended to mask a targeted cyber attack against Ukraine.
- It was aimed at Ukrainian infrastructures such as power companies, airports, the central bank and public transit.
- The attack was able to facilitate payment processing on a large scale for criminals, an illicit bitcoin exchange and money laundering across 75 shell companies and accounts globally.

Epsilon

- Epsilon – one of the world's largest email marketing service provider handling more than 40 billion emails and more than 2200 global brands landed up in a soup when hackers stole details belonging to more than 50 of their clients, including some top banks and retail giants!
- This data breach which was executed as a phishing email cost Epsilon over 4 billion USD.

Citibank

- The year 1995 saw Citibank in a string of slander when a criminal ringleader, Vladimir Levin, hacked the bank and illicitly transferred about 3.7 million USD into the bank accounts of his criminal organization.
- He executed this well-planned hack by using a computer that was based in London and a list of customer codes and passwords.
- He was finally tracked down by the FBI at a London airport.

Hannaford Bros.

- Hannaford, a supermarket chain with stores located mainly on the east coast of the US, fell prey to a security breach that exposed more than 4 million credit card numbers, leading to about 1800 cases of fraud in the year 2008.
- Having affected nearly 200 of its stores, the breach cost Hannaford over 250 million USD!

JP and Morgan Chase & Co

- In 2015, the accounts of 76 million households and 7 million small businesses associated with JPMorgan Chase were compromised in what the hackers described as “one of the largest thefts of financial-related data in history.
- The hackers then sold these personal data to a larger network of accomplices.
- Investigations later revealed that apart from personal data, the hackers also stole their business-critical data which enabled them to manipulate the company’s stock prices and make illicit financial profits.

LinkedIn Hacking

- Social networking website LinkedIn fell prey to a hack executed by Russian cyber criminals who stole the passwords of nearly 6.5 million user accounts.
- Soon these stolen passwords were made available in plain text on a Russian password forum!
- Adversity struck again when LinkedIn discovered in May 2016 that an additional 100 million compromised email addresses and passwords that were claimed to be from the 2012 breach, were released into the hacker forum.
- Some tech news reports have revealed that hackers were trying to sell this information on a darknet market for around $2200 each!

Online Culture

- Another group of studies about Internet cultural analyst focuses on is the social interaction that takes place in online social contexts such as forums, newsgroups and chats.
- A great deal of such Internet studies recalls anthropological theories and concepts to explain the emergence of community in that kind of online settings.
- The important issue here is not the technology itself, but the social interaction that occurs in cyberspace.
- David Porter, for example, in his introduction to Internet Culture, points out that communication through Internet can be understood from the perspective of culture since in virtual spaces one can find shared systems of believes, values and norms, specific ways of doing, a common understanding of symbols as emoticons, a netiquette and other signs that can perform a collective sense of belonging and create community.

- We can find here theoretical background linked to a holistic perspective of culture, such as the structural-functionalist approach, in the sense that a social group can be studied in isolation, as a complete cultural system.
- Margaret Mead and Culture and personality model has been used to some extend by the researchers to develop ethnographic oriented studies to describe virtual communities as if they were a new “tribe”.
- In fact, Elisabeth Reid - 1994- ethnography takes Geertz perspective to show how people involved in MUDs develops specific cultural forms as they create places, objects, subjects and actions, laws and social order, but over all, from these interactions emerge a sense of community and belonging of similar characteristics of offline social life.

*__MUDs-multi-user dungeon__, with later variants __multi-user dimension__ and __multi-user domain (Role Playing Video Games)__

- The counter part of these positions, most of which view Internet cultures as new cultural forms that elude offline social and cultural categories, allowing more democratic and collaborative models of social interaction in metaphysic communities, was the ethnographic work of Daniel Miller and Don Slater, which situated online practices in relation with people daily life in a concrete cultural context.
- People construct online collective identities, but these online interactions could not be understood only in terms of a specific disembodied “virtual” culture. In fact, they said, these online groups only make sense in relation to offline social, political and cultural contexts.
- Breaking with the online/offline, real/virtual dichotomies was very useful to begin to understand online interaction as a part of daily life activities, as a social practice.

Cultural Product

- Cyberculture can also be understood as the cultural production that use Internet and hypermedia tools to develop creative works of art, literature, music, etc.
- Culture is then associated with symbolic production, and also related, to much extend, with the western folk concept of culture as opposed to illiteracy, and meaning fine arts production.
- Cultural Studies have opened the "high" cultural production to popular culture, implying mass media production and consumption, but also current people crafts and appropriations of fine arts and media cultural products.
- These literary and media studies also brought a new perspective of analysis from formal and semiotic studies to the study of the social meaning of cultural representations in concrete social and historical contexts, an approach that finds useful some anthropological theories about culture, especially those related with symbolic practices, such as religion and myth.

- So, cyberculture is seen as the sum of cultural products developed and exchanged through Internet
- And the issues of research are, then, linked to the characteristics of these types of cultural production, distribution, regulation and consumption

- following Hall and du Gay model-, stressing their collaborative and interactive aspects

- and how people appropriated Internet technologies to express and to represent them selves

Media Form

- The next step is, to understand Internet as a media form. Internet can be seen as a media form in as much it is a communication technology that somehow develop and put together former communicative practices.
- Internet as a media form has also a relation with new modes of consumption. Internet, associated with other informational technologies, represents today a potential challenge to mass media and entertainment industries.
- Its technical feature developed since now, may not represent a serious challenge to mass media communication by itself, but it breaks the established circle of production, distribution and consumption regulated and dominated by big corporations, while others born for taking Internet advantages are arising.
- David Gaullnet reader, Web Studies, Rewiring media for the digital age, is an example of the kind of studies that relate intertextual media practices with topics such identity, representation, gender, ethnicity, political activism and new forms of sociality.

Conclusion

- Anthropological tradition in understanding human action and being through the concept of culture has proved to be implicitly used in almost all approaches to cyberculture, and if not, it has been useful to critically analyse such views and outputs.
- Christine Hine in her book Virtual Ethnography makes a distinction between cultural oriented studies about Internet use.
- On one hand, the approaches centered in the analysis of culture, on the other, these that cope with a cultural analysis of technology use.
- The firsts, take culture as an integrated whole that can be described from an observer point of view. The seconds, take an insider perspective, in the sense that any cultural description must be necessarily partial and situated, following the links of the network that conform our field of study, being the researcher part of the weave.

- Following this distinction, cyberculture as a new cultural model and the studies about culture formations in the Internet will fit the first option, while, Cyberculture as a cultural product of Internet use and as a media practice will follow a cultural analysis approach.
- Some scholars claim the necessity of a new anthropological specialty such as a Cyberanthropology (Budka), to deal with the new field of study of Cyberculture, which needs its own theoretical frame and methodology development.
- An example is the extension of the term “virtual ethnography”, meaning the adaptation of ethnography fieldwork to online social and cultural meaningful contexts.
- The term “cyberculture” could be redefined as a concept and could lead to an objectivation of cyberculture as a social phenomena or a cultural entity that exists independently of our theoretical gaze.

References

1. *Silver, David (February 2004). "Internet/Cyberculture/ Digital Culture/New Media/ Fill-in-the-Blank Studies". New Media & Society. **6** (1): 55–64. doi:10.1177/1461444804039915. ISSN 1461-4448. S2CID 32041186.*
2. ^ *"The digital language divide". labs.theguardian.com. Retrieved 2022-05-11.*
3. ^ *"Chart of the day: The internet has a language diversity problem". World Economic Forum. Retrieved 2022-05-11.*
4. ^ *Pogue, David (May 1995). "Mega 'Zines: Electronic Mac Mags make modems meaningful". Macworld: 143–144. The internet is one gigantic well-stocked fridge ready for raiding; for some strange reason, people go up there and just give stuff away.*
5. ^ Jump up to:[a] [b] *"cyberculture, n". OED online. Oxford University Press. December 2001.*
6. ^ *"cyberculture, n". American Heritage Dictionary of the English Language, Fourth Edition. Boston: Houghton Mifflin. 2000.*
7. ^ *Manovich, Lev (2003). "New Media from Borges to HTML" (PDF). In Noah Wardrip-Fruin, Nick Montfort (ed.). The New Media Reader. MIT Press. pp. 13–25. Retrieved 6 May 2007.*
8. ^ *Manovich, Lev (2001). The Language of a New Media. MIT Press. ISBN 0-262-63255-1.*
9. ^ *Forest, Fred. "Pour un art actuel, l'art à l'heure d'Internet". Retrieved 2008-02-15.*

10.^ *Macek, Jakub (2005). "Defining Cyberculture (v. 2)". Retrieved 2007-02-15.*
11.^ *Lister, David; Jon Dovey; Seth Giddings; Iain Grant; Kieran Kelly (2003). New Media: A Critical Introduction. Routledge. ISBN 0-415-22378-4.*
12.^ *Abate, Tom (29 September 2007). "High-tech culture of Silicon Valley originally formed around radio". SF Gate. Retrieved 18 January 2022.*
13.^ *Edwards, Benj (2016-11-04). "The Lost Civilization of Dial-Up Bulletin Board Systems". The Atlantic. Retrieved 2022-02-04.*
14.^ Jump up to: *Allebach, Nathan (2020-07-31). "A Brief History of Internet Culture and How Everything Became Absurd". The Startup. Retrieved 2022-02-04.*
15.^ Jump up to: *Friedman, Linda Weiser; Friedman, Hershey H. (2015-07-09). "Connectivity and Convergence: A Whimsical History of Internet Culture". Rochester, NY. SSRN 2628901.*
16.^ *"Google It! Jennifer Lopez Wears That Grammys Dress—The One That Broke the Internet—20 Years Later at Versace". Vogue. 2019-09-20. Retrieved 2022-02-04.*
17.^ *"COVID-19 changed global Internet culture, says app maker". Punch Newspapers. 2022-02-01. Retrieved 2022-02-04.*
18.^ *"Google Trends". Google Trends. Retrieved 2022-02-04.*
19.^ *"Framework for the Metaverse". MatthewBall.vc. Retrieved 2022-02-04.*
20.^ *"In the middle of a crisis, Facebook Inc. renames itself Meta". AP NEWS. 2021-10-28. Retrieved 2022-02-04.*

ww.tigweb.org/actiontools/projects/download/4926.doc https://www.tutorialspoint.com/information_security_cyber_law/introduction.htm

https://www.slideshare.net/bharadwajchetan/anintroduction-to-cyber-law-it-act-2000-india

https://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW

https://cybercrime.org.za/definition [6]http://vikaspedia.in/education/Digital%20Litercy/information-security/cyber-laws

https://www.ijarcsse.com/docs/papers/Volume_3/5_ May2013/V3I5-0374.pdf

https://www.livemint.com/technology/tech-news/how-india-became-a-hack-for-hire-hub-11595768182875.html

https://searchsecurity.techtarget.com/definition/emailspoofing

https://www.helplinelaw.com/employment-criminaland-labour/CDII/cyber-defamation-in-india.html