



THE CHARMS AND PERILS OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

CHRISTOPHER ALEXANDER UDOFIA

PHILOSOPHY DEPARTMENT, AKWA IBOM STATE UNIVERSITY

Abstract

This piece is an insightful reflection on the positive prospects and perils offered by the Information and Communication Technology (ICT) sector. The work will also highlight measures to be applied in addressing the perils that arise from the ICT. The objective of the research is to equip us with knowledge about the ICT so as enable us to utilize the ICT with the relevant caution. The work applies the philosophical research tools of exposition and critical analysis in the discussion of the benevolent and the malevolent dimensions of sector.

Key words: Information and Communication Technology, Charms, Perils, Benevolence, malevolent.

Introduction

The exponential surge in products and devices in the Information and Communication Technology sector has recorded unparalleled gargantuan use and patronage of ICT products and services. The products and services offered by the ICT range from computer and computer services, General System of Mobile Communication (GSM), Social media, internet services and applications *ad infinitum*. The enormous development milestones recorded in this sector is Lilliputian compared to the ever evolving unfathomable promises. The Internet, an octopus in this sector, was first created as a private research and communication network by the U.S. Army, exclusively used only for academic and military purposes between 1970 to 1980 and was privatized and commercialized in 1995. The problematic however, is that

amidst these benign charms and appeals of the ICT, there are horrible malicious perils and abuses that culminate in a phenomenon called Cyber Crime. This work shall attempt to discuss and contour the charms/benevolence and perils/malevolence of ICT and it shall proffer some provisional propositions for tackling the malevolent and perilous aspects of ICT.

Information and Communication Technology (ICT): Its Benevolent and Malevolent Dimensions.

Embedded in Cyber-technology are tremendously applaudable and benign as well as horrendously despicable and malicious potentials. The Jekyll and Hyde nature of ICT constitute the good and bad, the bright and dark and the use and abuse dimensions that characterize the cyber world. Information and Communication Technology (ICT) is used as an extended synonym for Information Technology (IT), and as a term it describes the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers, enterprise software, middleware, storage and visual systems, which enhance the assessment, storage, transmission and manipulation of information by users. ICT is also used to refer to the convergence of audio-visual telephone networks with computer networks through simple cabling or link systems ("Information and Computer Technology" en.m.wikipedia.org/wiki/Information-and-communications-technology). This specific and limited view of the ICT is commonly regarded as the Internet.

The Internet (literally, interconnection of computers through networks) is the interconnection of computers via wireless networks, telephone lines, cable and satellite connections for the purpose of transmitting information. The use of internet services cuts across all the facets of human endeavours. In the Academic and research sector, it serves as a tool of unprecedented enlightenment which has placed copious information at the disposal of researchers in all works of life. The World Wide Web service of the internet is intensely trafficked and utilized by researchers to access online resources which embellish their research perspectives. The magnitude of this traffic is corroborated by a study which shows that as at 2007, internet users were sharing 64,000 times over, the equivalent of the entire U.S. Library of Congress, on daily basis (Futerra, online).

The Commercial world and the Financial (Banking) industry have been widely transformed, courtesy of the internet. E – Commerce has enabled business transactions to transcend the traditional market interface and geographical cum cultural barriers. Physical cash transaction and its attendant danger have been greatly reduced by the introduction of Credit card mode of payment for goods and services. Business advertisement and communication are no more done with a local audience in focus but with a universal one. The Electronic Mailing system (E-mail) is a costless and expeditious system of mailing that has replaced the traditional Postal Agency. The social media form of communication has introduced a litany of cost-effective communication trends which have eradicated the encumbrances of the traditional trends.

It is not incongruous to assert that there is no facet of human life that is not either proximately or remotely determined and influenced by the ubiquitousness of this technology. Incontrovertibly, one can attest that it has reduced the universe into a *palmverse* and human life into an *e-life*. However, lurking in the escapades and benevolence of the ICT, nay, Internet, are perilous malevolent human and society manglers that manifest when this technology is abused. Abuses of the ICT and internet are pervasive employment of the embedded and manifest forces in a malevolent, disturbing, inordinate, immoral and illegal patterns. Technically, these abuses mostly lead to acts that constitute Cyber crimes (“crime on the Net” online). Net crime or internet crime refers to ‘offences that are committed against individuals or groups with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as internet (chat rooms, emails, notice boards and groups) and mobile phones (sms/mms) (“Computer Crime,” *Wikipedia*, online). Analyses of these criminal activities perpetrated via the Internet are:

1. **Hacking:** This act manifests in various forms, such as –
 - i. Breaking the security protocols of a network and accessing it without legitimate authorization.
 - ii. Defacing the content of another’s website.
 - iii. Diverting others access to a particular website.
 - iv. Slowing down the speed of a server by overwhelming it with heavy messages.
 - v. Denying a site’s service to other users.

In February 2000, a hacker denied the services of Yahoo, CNN, eBay, Buy.com, Amazon, E Trade, Datek and 2DNet to users by hacking into 75 computers in different networks from which he used to attack 11 internet sites. The culprit which was called Mafia boy was apprehended and sentenced. Numerous hacking occur on daily basis, mostly by mercenaries who try to obtain the credit card details of people so as to perform illegal transaction with them.

The phone-hacking saga otherwise called –“Hackgate”, “Rupertgate or “Murdochgate” (“News_International Phone Hacking Scandal,” *Wikipedia*, online) was a raging controversial scandal that involves the media mogul Rupert Murdoch and his media business. His best- selling weekly British tabloid, *News of the World*, was entangled in accusations of hacking into the telephones of Iraq and Afghanistan war veterans, murder victims and their families. It is also alleged to have hacked into the voice mail of the 13 year old, Late Milly Dowler. The abduction of Milly led to her parents sending desperate voice messages to her phone. The tabloid monitored and retrieved the voice mails from the parents without the parents’ consent. When the box was full, the paper deleted some mails so as to allow space for more. This deletion created the misrepresentation to the abducted parents and friends that Milly is still alive and must have done the deletion.

2. **Viruses:** They are in three forms namely-
- i. **Virus** – This is a malicious code which can erase files or lock up a system. It attaches itself to files and computer programmes.
 - ii. **Worm** – This form does not attach itself to files or programmes but rather infiltrates a network.
 - iii. **Trojan horse-** This programme performs destructive functions in the pretext of doing something innocuous.

It is projected that about 20,000 viruses that destroy computer programmes have been created in addition to the daily proliferation of potentially destructive mutations. Many businesses have been adversely battered by the infection of viruses. The year 2000 computer crash was caused by the Love Bug virus and it affected about 45 million people in a one day swoop at a damage cost pegged at 8.75 billion.

3. **Pirating:** The ICT has provided a prolific facility and framework for illegitimate proliferation and violation of intellectual properties and the accompanying rights. The copying and the sharing of peoples' creations such as scholarly publications, films, music etc. using ICT devices constitute a gross violation of intellectual property right.

4. **Illegal Trading:** The ICT has offered hoaxers the fertile arena for engaging in illegal transactions by impersonating original producers and counterfeiting their products. A deluge of goods are advertised online which lack credible certification by reliable certifying and quality assurance agencies.

5. **Fraud:** Nuhu Ribadu ("Cybercrime and Commercial Fraud: A Nigerian Perspective") enunciates the fraudulent schemes committed through the instrumentality of the internet to include contract scam, credit card scam, inheritance scam, lottery scam, currency scam, marriage scam, immigration scam, counterfeiting, religious scam etc. The advancement of ICT has enabled a surreptitious and ubiquitous plotting and actualization of a barrage of crimes. The practice of phishing" – a scam in which emails purportedly coming from one's banks demand the clients to forward to certain addresses their private banking details and other sensitive information like personal pin number (PIN) credit card number, bank account number, social security number etc is on the increase daily. The brand of online fraud originating from Nigeria is dubbed, the Nigerian 419" scam. Section 419 of the Nigerian Criminal Law Act deals with a number of fraudulent offences hence, the description 419 is a reference to those offences which are proscribed by section 419 of the Criminal Law Act of Nigeria. This phenomenon was overtly prevalent in the Nigerian society as a fast track for making mega-bugs that Christopher F. Chabris and Daniel Simians ("How to Beat Nigerian Scams") observe that if one types "Nigerian" into Google, one was always sure to get, as one of the key suggestions, "scam". One of the common threads of this scam, was an unsolicited email proposing a mouth watering return on investment or facilitation of the process.

6. **Libel:** The internet is also used as an interface for posting unsubstantiated defamatory information. Recently, a publication containing the ominous malicious news of the death of Nelson Mandela was flashed on the net, the internet is replete with such unsubstantiated news and allegations not grounded on solid facts.
7. **Cyber Terrorism:** Terrorists have learned how to manipulate the net to post threats and attacks. One of the ways of Cyber terrorism is the hacking of national or organizational security and defense intelligence. Other forms include the online publication of threats by terrorist group to coerce a government or an organization into compromises and concessions.
8. **Pornography, Obscene and offensive contents:** The ICT is used by many for engaging in a number of illicit acts like posting and viewing of sex videos and nude pictures, inordinate chatting, obscene advances, propagating racial hate, sexual harassment of children and adult, human trafficking, fanaticism, bigotry, sectarianism, chauvinism etc. Pedophiles use the media of ICT to hoodwink minors, while rabid lechers exploit the content of ICT to aggravate and satiate their maniacal tendency by posting lewd videos, pictures and messages.
9. **Money Laundering:** Copious sums of money from dubious and illegitimate sources are transited without the requisite legal validation, via online banking and trading. Corrupt persons engage in this sort of transaction so as to short circuit and circumvent the legal rubrics which prohibit illegal money transfers and business transactions.
10. **Personality Disorder and ICT Devices Addiction:** The craving for and sordid dependence on the internet and other ICT devices have disoriented the personality of many. The prevailing obsessive attachment to ICT is causative of some of the morbid personality disorders and expressions. Such maniacal obsession with the ICT has resulted in some people wearing ear phones compulsively regardless of the damage unguarded usage may cause to health.

Many relationships and pursuits have been ruptured due to party's chronic attachment to ICT which causes the actualization of the relationship and accomplishment of pursuits to be jeopardized. People's pre-occupation with mobile communication devices has resulted in profane and sacrilegious act like making and answering phone calls, pinging, texting etc. in sacred places during sacred liturgies.

Tackling the Perils of ICT

1. The prevention of ICT abuse and cyber crime requires vigilance from the users. ICT users must not divulge personal information like full name, ATM pin, credit card details, social security number, account numbers etc to unknown and suspicious recipients.
2. Enactment and promulgation of unequivocal ICT policies and regulations will go a long way in taming ICT abuses and crimes. It is fundamental that nations should enact and implement laws and policies guarding ICT use. A major reinforcement to internet crime is the non-existence of cyber crime statutes. There is need for the creation of cyber-regulations and statutes both at the national and international levels, if cyber abuse must be curbed.

3. Effective ICT policing is a sine qua non for the prevention of ICT crimes. The crime fighting agencies at the local and international levels must engage in vigorous training so as to be adept with the latest trends on criminal internet abuse and conceive measures ways of combating them.
4. There is urgent need for a concerted moral crusade in our societies. ICT crimes are mostly borne out of a morally debased consciousness. The moral profile of the cyber crime offenders and perpetrators are disreputable, but that of most victims is equally bankrupt because most of the victims become easy preys due to their gullibility to inordinate and illegitimate gains.

Conclusion

The development and advancement of Information and Communication Technology constitute an innocuous and ingenious adventure which possess the inherent paradoxical capacities for use and abuse, benignity and malignity. ICT has evolved into a tremendous practical tool for overcoming and transforming hitherto unfathomable challenges. The advent of ICT has pushed back the frontiers of knowledge with an attendant profuse expository entries on all conceivable ideas and subjects. It has inaugurated a communication process that transcends the barriers of geography and culture, its impact in the business sector has diffused and eclipsed the hassles that were militating against the globalization and rectification of commercial activities to attend to the exigencies of the era. In manufacturing and industry, every activity in these areas has had a touched of refinement courtesy of the unprecedented facilitation of ICT.

There is hardly any aspect of human existence that the ubiquitous ICT has not transcended. Just like the advantages and uses of ICT crescendo *ad infinitum* its proclivity for conversion into a mechanism for the perpetuation of horrendous and malicious activities is outlandish and bizarre. This grotesque development exposes the ironies and contradictions accompanying the evolution and development of the ICT. The imminent danger haunting humanity as a consequence of these internecine contradictions of ICT is the possibility of the concoction of today's ICT advancement into an annihilation time bomb whose unpredictable detonation can reverse human society and retrogress our copious progress to that of bestial renegades and innuendos.

Works Cited

Chabris, C. F and Simons, D. "How to Beat Nigerian Scams", *The Wall Street Journal*, U.S Edition, onlinewsj.com/article /SBI00. Friday, August, 2012.

Comer, Douglas E. "Internet," *Microsoft Encarta*, 2009 [DVD]

Futerra. "Facing up to Extreme Abuse of the Internet." chris.tuppen@bt.com, May, 2004.

Ribadu, Nuhu. "Cybercrime and Commercial Fraud: A Nigerian Perspective," *Modern Law for Global Commerce Congress to Celebrate the Fortieth Annual Session of UNCITRAL*, Vienna, 9-12 July, 2007, 3.

Roger Darlington. "Crime on the Internet." www.rogerdarlington.me.uk/crimeonthenet.html

Wikipedia. "Information and Computer Technology," en.m.wikipedia.org/wiki/Information-and-communications-technology.

-----"Computer Crime," en.m.wikipedia.org/wiki/computer_crime.

-----"News International Phone Hacking Scandal," [http://en.wikipedia.org/ News_international phone_hacking_scandal](http://en.wikipedia.org/News_international_phone_hacking_scandal).

