COMPUTER ETHICS, CYBERNETICS AND CYBERCRIME INFORMATION IN NIGERIA

***AUWAL MAGAJI ABUBAKAR; **HAUWA MAMMAN SALEH; & ***SAHANATU MUAZU**

*Department of library and Information Science, Kaduna Polytechnic, Kaduna. **Department of Library and Information Services, Nigerian Institute of leather and Science Technology Samaru, Zaria. ***Department of Library and Information Services, Nigerian Institute of leather and Science Technology Samaru, Zaria.

Abstract

This study critically examines and explains key concepts that defines the new information age. These concepts include knowledge economy, information and knowledge society, cyber citizen, cyber warfare, information poverty and cyber bullying. The study also outlines possible strategies that could protect information users form possible cyber bullying in addition to describing strategies that could promote good cyber citizens. Lastly, the study takes a look at some of the techniques that could be used in controlling cybercrime and cyber warfare and also outlines possible international computer and cybernetics ethics.

INTRODUCTION

Ethics is a set of moral principles that govern the behavior of a group or individual. Kidder (2003) states that "standard definitions of ethics have typically included such phrases as 'the science of the ideal human character' or 'the science of moral duty'". Similarly, Paul, R. and Elder, L. (2006), define ethics as "a set of concepts and principles that guide us in determining what behavior helps or harms sentient creatures". Computer ethics therefore, can simply be referred to as set of moral principles that regulate the use of computers. Some common issues of computer ethics include intellectual property rights (such as copyrighted electronic content), privacy concerns, and how computers affect society. Computer ethics is a concept in ethics that addresses the ethical issues and constraints that arise from the use of computers, and how they can be mitigated or prevented. This basically deals with the procedures, values and practices that govern the process of consuming computing technology and its related disciplines without damaging or violating the moral values and beliefs of any individual, organization or entity. Computer ethics primarily enforces the ethical implementation and use of computing resources. It includes methods and procedures to avoid infringing copyrights, trademarks and the unauthorized distribution of digital content. Computer ethics also entails the behavior and approach of a human operator, workplace ethics and compliance with the ethical standards that surround computer use. The core issues surrounding computer ethics are based on the scenarios arising from the use of the Internet, such as Internet privacy, the publication of copyrighted content and user interaction with websites, software and related services.

As technology advances, computers continue to have a greater impact on society. Therefore, computer ethics promotes the discussion of how much influence computers should have in areas such as artificial

intelligence and human communication. As the world of computers evolves, computer ethics continues to create ethical standards that address new issues raised by new technologies.

The term "computer ethics" was not commonly used until the mid-1970s when Walter Maner defined this field of study as one that examines "ethical problems aggravated, transformed or created by computer technology." Some old ethical problems, he said, were made worse by computers, while others came into existence because of computer technology. He suggested that we should use traditional ethical theories of philosophers, such as the utilitarian ethics of the English philosophers Jeremy Bentham and John Stuart Mill, or the rationalist ethics of the German philosopher Immanuel Kant.

In the same way, Johnson, D (1985) in her book, *Computer Ethics*, defined the field as one which studies the way in which computers "pose new versions of standard moral problems and moral dilemmas, exacerbating the old problems, and forcing us to apply ordinary moral norms in uncharted realms,". Like Maner before her, Johnson recommended the "applied ethics" approach of using procedures and concepts from utilitarianism and Kantianism but unlike Maner, she did not believe that computers create wholly new moral problems. Rather, she thought that computers gave a "new twist" to old ethical issues which were already well known.

James Moor's definition of computer ethics in his article "What Is Computer Ethics?" (Moor, 1985) was much broader and more wide-ranging than that of Maner or Johnson. He defined computer ethics as a field concerned with "policy vacuums" and "conceptual muddles" regarding the social and ethical use of information technology:

"A typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used. Computers provide us with new capabilities and these in turn give us new choices for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate. A central task of computer ethics is to determine what we should do in such cases, that is, formulate policies to guide our actions.… One difficulty is that along with a policy vacuum there is often a conceptual vacuum. Although a problem in computer ethics may seem clear initially, a little reflection reveals a conceptual muddle. What is needed in such cases is an analysis that provides a coherent conceptual framework within which to formulate a policy for action" (Moor, 1985, 266).

CYBERNETICS

The term cybernetics according to the Cambridge dictionary simply means the "scientific study of how information is communicated in machines and electronic devices, compared to how information is communicated in the brain and nervous system.

According to (Mindell, 2000) "Cybernetics is the study of human/machine interaction guided by the principle that numerous different types of systems can be studied according to principles of feedback, control, and communications". It is characterized by a tendency to universalize the notion of feedback, seeing it as the underlying principle of the technological world.

NEW INFORMATION AGE:KNOWLEDGE ECONOMY

A knowledge-based economy relies primarily on the use of ideas rather than physical abilities and on the application of technology rather than the transformation of raw materials or the exploitation of cheap labor. It is an economy in which knowledge is created, acquired, transmitted, and used more effectively by individuals, enterprises, organizations, and communities to promote economic and social

development (World Bank Insti-tute 2001c; World Bank 1998d). Knowledge can either be codified and written down or tacit and in people's heads

The World Bank Institute offers a formal definition of a knowledge economy "as one that creates, disseminates, and uses knowledge to enhance its growth and development". A knowledge economy uses data as it raw material and transforms it using technology, analysis tools, and human intelligence into useful applications for businesses that lead to economic (productivity) growth. Knowledge can be obtained and trained by experience, familiarity, science or learning. Often knowledge is taken together with innovation, the commercial exploitation of knowledge. Knowledge then is the adding up of abilities (capabilities, creativity and persistency) to recognize and solve problems, by collecting, selecting and interpreting information.

The knowledge economy refers to the knowledge work-based economy. The idea of knowledge work has been around for some time. Mintzberg (1983, in Garrick and Clegg, 2000, p 279) wrote extensively about knowledge intensive firms, outlining differences between knowledge intensive organizations and professional bureaucracies. In essence, this means (according to Shanhong, 2000) that the knowledge economy era is driven by a company's, and in effect an individual's, ability to effectively identify, acquire, develop, resolve, use, store, and share knowledge. It is also driven by the ability to apply the tasks listed above to create an approach to:

- transform and share both tacit and explicit knowledge;
- raise innovation capability; and
- utilize the combined wisdom of the team.
- According to World Bank Institute (2001) knowledge economy rests on four pillars
- A supportive economic and institutional regime to provide incentives for the efficient use of existing and new knowledge and the flourishing of entrepreneurship.
- An educated and skilled population to create, share, and use knowl-edge.
- A dynamic information infrastructure to facilitate the effective com-munication, dissemination, and processing of information.
- An efficient innovation system of firms, research centers, universities, consultants, and other organizations to tap into the growing stock ofglobal knowledge, assimilate and adapt it to local needs, and create new technology

INFORMATION SOCIETY

Information Society is defined as a society based on information and knowledge. Information society is an evolving concept and it is now at its youth. Presently, islands of information societies are taking shaped here and there. This is the early stage of information society. It will evolve, as the information age unfolds, and all these islands will join together, forming the Global Information Society.

Some of the very basic characteristics of information society are as follows:

- Information society is global in principle, for geographic borders are not recognized by the flow of information. It is, therefore, not our choice that the isolated information societies currently being developed in different parts of the world are going to join together, forming the Global Information Society. It is the natural trend in the evolution of information society.

- Information society demands and promotes clarity, precision, honesty, and openness. Dishonest politicians and officials cannot survive in this society. They can no longer fool citizens by false stories, for a wealth of information would be available for every citizen, who can simply look up and discover the facts. It is now clear for almost everyone, for example, that "the treat of terrorism or weapons of mass destruction" is nothing but a propaganda for the US invasion of Iraq.
- Information society is governed by knowledge, competence, and only informed decisions and actions. There will be no room for incompetence in this society. The wealth of information and knowledge available for the citizens of information society provide an environment, where only informed, knowledgeable, and competent individuals can survive as managers and leaders of the society.
- Information society is a new environment, a new game, and a whole new set of rules. We must learn the rules and play the game by the rules. Those who cannot adapt to the new environment or violate the rules will not survive. In the example above, replacing a perfectly qualified and competent department head by an unqualified and incompetent one is a clear violation of the rules and, theoretically, must be rejected by the information society.
- Information society promotes equal opportunity. It has been a well-known fact since long time ago that "information is power." The free flow of information, in the information society, therefore, translates to equal distribution of power in this society. The availability of information to everyone without any restriction, control, or filtering, provides equal opportunity for all the citizens of information society.

KNOWLEDGE SOCIETY

The term knowledge society simply refers to the society in which the creation, dissemination and utilization of information and knowledge has become the most important factor of production. In such a society, knowledge is the most powerful asset for the production of wealth, sidelining the importance of land, the volume of labor and physical or financial capital.

According to (Ashikuzzaman, 2013) a knowledge society is a formal association of people with similar interest, who try to make effective use of their combined knowledge about their area of interest and in the process contribute to this knowledge.

The term knowledge society is used interchangeably with concepts such as knowledge-based economy, information society and knowledge driven economies.

A knowledge society generates, shares and makes available to all members of the society knowledge that may be used to improve the human condition. A knowledge society differs from an information society in that the former serves to transform information into resources that allow society to take effective action while the latter only creates and disseminates the raw data.

Knowledge Society is a term to describe societies which are economically and culturally characterised by a high degree of dependency on their potentials to create scientific and technological knowledge. Based upon the data-processing technologies in the information age a typical element is using knowledge strategically as a factor of economic competition among nations as well as among companies and services inside nations. Therefore research and development (R&D) are strongly connected. Knowledge is

becoming a special good in the market and a product to merchandise. In an economical view knowledge societies invest in education and training of people in order to build up resources of human capital which should enable them to fulfil expectations to perpetuate traditions and more important use the knowledge to develop innovations. In order to distinguish differences in quality of knowledge and knowledge institutions there is a high interest in ranking educational efforts. Social status of individuals is strongly dependent on the degree of their educational achievement. As an expression of late modernity knowledge societies are characterised by a reflexive conscience about the constructional and methodological processes.

A crucial attribute of knowledge society is an extraordinary increase of complexity of knowledge which affects not only one country but the whole world. Supported by high speed communication (internet) the amount of information cannot be coped by individuals only but has to be accompanied by educational curriculums and strategies to distinguish the meaning of information and to find a personal attitude to complexity of knowledge.

CYBER CITIZEN?

A citizen is simply a person who is a member of a particular country and who has right because of being born there or because of being given rights, or a person who lives in a particular town or city, hence the term "cybercitizen" simply means a “citizen of the cyberspace”, "citizen of the Internet" or a member of the "cybercommunity."A cyber citizen utilizes technology in an appropriate manner including etiquette, communication, education, access, commerce, responsibility, rights, safety and security.

CYBER WARFARE:

The digital world has brought exciting new era of technology but has also brought about several types of issues among which is the cyberwarfare. Since information technology and the internet have developed to such an extent that they have become a major element of national power, cyberwar has become a very serious issue as nation-states are arming themselves for the cyber battlespace.

The research community have offered many deferring definitions of cyber warfare and these includes the following:

Hopping, (2018) defined cyber warfare as the use of technology to launch attacks on nations, governments and citizens, causing comparable harm to actual warfare using weaponry.

Similarly, (Cornish et al., 2012) are of the opinion that “Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target.” The term ‘cyberwar’ has become a frequently used slogan to refer to any kind of conflict in the cyberspace with an international dimension.

INFORMATION POVERTY

One of the biggest challenges facing the world today is that of information poverty which and this can have a huge negative effect on the economic, cultural and socio-political development of nations if not properly addressed. Although, the concept of information poverty was officially used for the first time during the 1950s, the experience of being information poor is not new. However, Freeman & Louca (2002) noted that a new dimension was added to the notion of information poverty with the

transition to the information era. The transition, supported by the development of information and communications technologies (ICTs), brought about a globalized information-driven economy, also referred to as the knowledge economy, based on intellectual, intangible assets. Information poverty is furthermore not only of a political, cultural and socio-economic nature. We livein a new emerging global information society where we are, more than ever before, dependent on the creation, accessing, sharing and manipulation of information. This brings forward questions and concerns such as the fundamental freedom of people, the right to freedom of expression and to communicate, the right of access to information and the fair distribution of information in the market place. This emerging global information society and the growing divide between the information haves and information have-nots is therefore also a serious moral concern.

Although the definition and use of information poverty has developed since the development of ICT, Lievrouw and Farb correctly point out that the debate on information poverty has been overshadowed in the last decade by the growing importance of ICT. ICT played a dominant role in dividing the world between the information haves and the information have-nots, and should therefore not be underestimated, information poverty is not restricted or limited to a technology/digital divide only. The information divide is not limited to the 'technology insiders' and 'technology outsiders' of cyberspace.

Hence Britz (2004) defined "Information poverty as that situation in which individuals and communities, within a given context, do not have the requisite skills, abilities or material means to obtain efficient access to information, interpret it and apply it appropriately. It is further characterized by a lack of essential information and a poorly developed information infrastructure".

CYBER BULLYING

Cyberbullying, which is sometimes referred to as online social cruelty or electronic bullying, has been defined as "an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself" (Smith et al., 2008).

Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior.

Cyberbullying can involve:

- Sending mean, vulgar, or threatening messages or images
- Posting sensitive, private information and/or lies about another person
- Pretending to be someone else in order to make that person look bad
- Intentionally excluding someone from an online group (Willard, 2007)

CYBER BULLYING ORCHESTRATED BEHIND CYBER WALLS;STRATEGIES FOR PREVENTION

No one should have to endure cyberbullying. It leaves children and teens frightened, upset, and perplexed. They tend to not know why this attack is happening to them and often are unsure as to who can help them resolve this troublesome and often scary situation. Combined efforts of school and home are needed to prevent, reduce, or eliminate cyberbullying

What Can Victims Do?

Victims of cyberbullying should not retaliate, as this may promote more intensive harassment from the cyberbully and may make it unclear as to who originally instigated this aggressive, hurtful behavior.

All victims of this type of behavior need to alert a responsible adult or appropriate authorities as soon as it occurs. Depending on the severity of the cyberbullying, the following steps should be considered by victims and their parents:

i. Calmly and strongly tell the cyberbully to stop the harassing behavior and remove any offensive material from future communications.
ii. Ignore or block the communications.
iii. Make a hard copy of the material the cyberbully has posted and send it to the cyberbully's parents to solicit their help in ceasing this problematic behavior.
iv. Clean up the instant messaging buddy list to help reduce the number of other people who have access to the victim's e-mail location.
v. File a complaint with the website, Internet service provider (ISP), or cell phone company.
vi. Enlist the help of the school psychologist, school counselor, principal, or school/police liaison officer.
vii. Contact an attorney if less drastic steps are ineffective.
viii. Contact the police if the cyberbullying includes threats of harm.

How Can Parents Help Prevent Cyberbullying? Since cyberbullying occurs most often while children and adolescents are at home, parents can be a great resource in preventing instances of this type of bullying. The following steps should be considered:

i. Keep home computer(s) in easily viewable places, such as the family room or kitchen.
ii. Talk regularly with children about their online activities and Internet etiquette in general.
iii. Talk specifically about cyberbullying and encourage children to notify adults immediately if they become victims of cyberbullying.
iv. Tell children that you may review their online communications if there is any reason for concern.
v. Help children understand that cyberbullying is harmful and unacceptable behavior.
vi. Emphasize expectations for responsible online behavior and make clear the consequences for violations of Internet etiquette.
vii. Consider establishing a parent–child Internet use contract.
viii. Beware of warning signs that might indicate the child is being bullied, such as reluctance to use the computer, a change in the child's behavior and mood, and/or reluctance to go to school.
ix. Consider installing parental control filtering software and/or tracking programs, but do not rely solely on these tools.
x. Encourage antibullying legislation and Internet safety policies at the state, local, and district levels. Many states have enacted antibullying laws that address all forms of bullying in schools. Further, some school

Educators should determine the prevalence of cyberbullying, conduct a threat assessment in response to reports of cyberbullying that might involve violence or suicidal behaviors, and develop programs, policies, and training to prevent and stop cyberbullying on campus.

- Conduct a cyberbullying needs assessment to identify the incidence of cyberbullying in the school, including where it occurs and any factors that discourage reporting. This might involve creating a survey and distributing it to teachers, administrators, and parents. The results can be analyzed and used to pinpoint areas of concern. It might also be a good idea to conduct a structured interview with the principal to obtain more information about the school's needs and the principal's goals with regard to cyberbullying.
- Make a plan to implement a threat assessment for any report of cyberbullying that raises concerns about the possibility of violence or suicide.

- Include cyberbullying in the school's comprehensive antibullying program to educate students and ensure that all personnel respond appropriately when cyberbullying is reported. Review written policies related to students' use of the Internet and mobile communication devices to ensure that they address on-campus cyberbullying. Also review the district's Internet use policies to ensure effective student supervision and monitoring.
- Provide colleagues, parents, students, and community members with information about preventing and responding to cyberbullying. Faculty and staff should also be trained in early warning signs that may identify victims of cyberbullying, including rejection or isolation from peers and being the focus of more traditional forms of bullying. Be adamant about looking for the circulation of pictures, video clips, sound files, and any other items used to ridicule and defame students' characters.

GOOD CYBER CITIZENS.

a) Be a good digital citizen. The things that you would not do in your physical life, do not do in your digital life. If you see crime online, report it the same way that you would in real life. Keep yourself safe and assist in keeping others safe on the Internet.
Respect yourself and others. Practice good netiquette, know the law, and do not do things that would cause others harm. The Golden Rule applies online, as well.
b) Practice good communications. Never send an e-mail typed in anger. Put it in your draft folder and wait. Keep in mind that digital communications do not give the reader the same visual or audio cues that speaking in person (or by video or phone) does.
c) Use antivirus and antispyware software. The use of antivirus and antispyware will help prevent spyware and malware on your devices.
d) Understand the technology available to protect your digital identity. Digital security devices give you the freedom to communicate, shop, bank and work using your digital identity in a way that is convenient and secure.
e) Consider using a personal security device when going online. Having a personal security device in addition to a password better secures you and your sensitive information.
f) Report cybercrime.
g) Do not share information with websites you do not trust. If you are not sure about a website, look to see if it is certified by an Internet Trust Organization such as the Better Business Bureau (BBB Online), TRUSTe and WebTrust.
h) Protect your home or small business Wi-Fi network, you can do this by implementing the authentication security capabilities built into your access points and wi-fi adapters.

CONTROLLING CYBERCRIME AND CYBER WARFARE

Access to your personal information is what gives hackers the power to tap into your accounts and steal your money or your identity. But the right information can also empower you to protect yourself from being caught up in the thriving industry that is cybercrime.

- Education: By educating yourself about the types of scams that exist on the Internet and how to avert them, you are putting yourself one step ahead of the cybercriminals. Learn about cybercrime and talk to your family about how to identify scams. Never give out your personal information to anyone you do not know on the Web.
- Use a firewall - Firewalls monitor traffic between your computer or network and the Internet and serve as a great first line of defense when it comes to keeping intruders out. Make sure to use the firewall that comes with your security software. And if you have a home wireless network, enable the firewall that comes with your router.

- Practice safe surfing - When navigating the web, you need to take precautions to avoid phony websites that ask for your personal information and pages that contain malware. Use a search engine to help you navigate to the correct web address since it will correct misspellings. That way, you won't wind up on a fake page at a commonly misspelled address.
- Use comprehensive security software and keep your system updated Purchase and install anti-virus software such as McAfee or Norton Anti-Virus. AVG offers free anti-virus protection if you do not wish to purchase software.
- Shop only at secure websites. Look for a Truste or VeriSign seal when checking out. Never give your credit card information to a website that looks suspicious or to someone you don't know.
- Use strong passwords on your accounts that are difficult to guess. Include both letters and numerals in your passwords. Never use a word that is easy to guess -- like your wife's name, birthdays, phone number etc.
- Use common sense - Despite the warnings, cybercrime is increasing, fueled by common mistakes people make such as responding to spam and downloading attachments from people they don't know. So, use common sense whenever you're on the Internet. Never post personal information online or share sensitive information such as your social security number and credit card number. Exercise caution when clicking on any links or downloading any programs.
- Be suspicious - Even if you consider yourself cyber savvy, you still need to keep your guard up for any new tricks and be proactive about your safety. Backup your data regularly in case anything goes wrong, and monitor your accounts and credit reports to make sure that a hacker has not stolen your information or identity.
- Keep watch over your children and how they use the Internet. Install parental control software to limit where they can surf.

OUTLINE OF THE POSSIBLE INTERNATIONAL COMPUTER AND CYBERNETICS ETHICS

The **Ten Commandments of Computer Ethics** were created in 1992 by the Computer Ethics Institute. The commandments were introduced in the paper "In Pursuit of a 'Ten Commandments' for Computer Ethics" by Ramon C. Barquin as a means to create "a set of standards to guide and instruct people in the ethical use of computers." They follow the Internet Advisory Board's memo on ethics from 1987. The Ten Commandments of Computer Ethics copies the style of the Ten Commandments from the King James Bible.

The Ten Commandments of Computer Ethics

1) Thou shalt not use a computer to harm other people.
2) Thou shalt not interfere with other people's computer work.
3) Thou shalt not snoop around in other people's computer files.
4) Thou shalt not use a computer to steal.
5) Thou shalt not use a computer to bear false witness.
6) Thou shalt not copy or use proprietary software for which you have not paid (without permission).
7) Thou shalt not use other people's computer resources without authorization or proper compensation.
8) Thou shalt not appropriate other people's intellectual output.
9) Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10) Thou shalt always use a computer in ways that ensure consideration and respect for other humans.

References:

Ashikuzzaman, M. (2013). *Knowledge society definition - Library & Information Science Network*. http://www.lisbdnet.com/knowledge-society-definition/

Barquin, Ramon C. (May 7, 1992). "*In pursuit of 'Ten Commandments' for Computer Ethics*". *Computer Ethics Institute*. http://computerethicsinstitute.org/barquinpursuit1992.html Retrieved 10-02-2020.

Britz, J. J. (2004). To Know or not to Know: A Moral Reflection on Information Poverty. *Journal of Information Science, 30*(3), 192-204. doi:10.1177/0165551504044666

Castelfranchi, C. (2007). Six critical remarks on science and the construction of the knowledge society. Journal of Science Communication, 6(4), 1-3.

Chatman, E. A. (1991). Life in a Small World: Applicability of Gratification Theory to Information-Seeking Behavior. *Journal of the American Society for Information Science (1986-1998), 42*(6), 438.

Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2012). On Cyber warfare. In *Encyclopedia of Cyber Behavior* (Vol. 1, pp. 1074–1087). https://doi.org/10.4018/978-1-4666-0315-8.ch088

Freeman, C., & Louca, F. (2002). As Time Goes By: From the Industrial Revolutions to the Information Revolution. : Oxford University Press. Retrieved 17 Feb. 2020, from https://www.oxfordscholarship.com/view/10.1093/0199251053.001.0001/acprof-9780199251056.

Hopping, C. & W. D. (2018). *What is cyber warfare? | IT PRO*. ITPro. https://www.itpro.co.uk/security/28170/what-is-cyber-warfare

Johnson, D. G. (1985) Computer Ethics, Prentice-Hall, 2nd Edition, 1994.

Kidder, R. (2003).How Good People MakeTough Choices: Resolving the Diliemmas of Ethical Living.New York:Harper Collins. p. 63.ISBN0-688-17590-2.

L.A. Lievrouw and S.E. Farb, Information and equity. In: B. Cronin (ed.), Annual Review of Information Science and Technology (ARIST), Vol. 37 (Information Today, Medford, 2003) 499–538.

Maner, Walter (1980) Starter Kit in Computer Ethics, Helvetia Press (published in cooperation with the National Information and Resource Center for Teaching Philosophy). [Originally self-published by Maner in 1978.]

Mindell, D. A. (2000). Cybernetics: Knowledge domains in Engineering systems. *Origins*, 1–7. http://web.mit.edu/esd.83/www/notebook/Cybernetics.PDF

Moor, James H. (1985) "What Is Computer Ethics?" In Bynum, Terrell Ward, ed. (1985) Computers and Ethics, Blackwell, 266-75. [Published as the October 1985 issue of Metaphilosophy.]

O'Reilly, Dennis (October 12, 2010). "*The Internet and the death of ethics*". *CNET*. https://www.cnet.com/news/the-internet-and-the-death-of-ethics/ Retrieved February 10, 2020.

Paul, R. and Elder, L. (2006). The Miniature Guideto Understanding the Foundations of Ethical Reasoning.United States: Foundation for Critical Thinking FreePress. p. np.ISBN0-944583-17-2.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49, 376-385.

The Ten Commandments of Computer Ethics" *(PDF). Retrieved* 2012-05-22.

Willard, N. (2007). *Cyber bullying and cyberthreats: Responding to the challenge of online social cruelty, threats, and distress.* Champaign, IL, Research Press.

World Bank (2009). The Knowledge Assessment Methodology (KAM) website (www.worldbank.org/kam)