International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 1, January-February 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cyber Ethics: An Introduction

Paul A. Adekunte[1], Matthew N. O. Sadiku[2], Janet O. Sadiku[3]

[1]International Institute of Professional Security, Lagos, Nigeria
[2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, Texas, USA
[3]Juliana King University, Houston, Texas, USA

ABSTRACT

Cyber ethics is the study of the ethics relating to computers, as well as to user behavior and what computers are programmed to do, and how it affects individuals and society. It is the branch of philosophy that deals with what is considered to be right or wrong. Since the advent of computers, various governments have enacted regulations and while organizations have defined policies about cyberethics. Cyberethics also known as "internet ethics," is a branch of applied ethics that examines the moral, legal, and social issues (i.e. ethical questions) brought about by the emergence of digital technologies and global virtual environments. Arising with the introduction of the internet are, filtering, accuracy, security, censorship, conflicts over privacy, property, accessibility, and others. This paper is to elucidate more on cyberethics and its impacts on users and the society.

KEYWORDS: *cyberspace, moral rules, code of behavior, online environment, cyber society, cybercrime, cybersecurity, ransonware*

How to cite this paper: Paul A. Adekunte | Matthew N. O. Sadiku | Janet O. Sadiku "Cyber Ethics: An Introduction" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-1, February 2024, pp.816-822, URL: www.ijtsrd.com/papers/ijtsrd63513.pdf

IJTSRD63513

WHAT IS CYBERETHICS?

Cyberethics refers to a set of moral rules or a code of behavior applied to the online environment. As a responsible netizen, one should observe these rules to help make the cyberspace a safe place. Cyberethics is a branch of applied ethics that examines the impact that the moral, legal, and social issues have at the intersection of computer/information and communication technologies. This is also referred to as internet ethics, computer ethics, and information ethics [1, 2]. Computer ethics is a field of applied ethics that addresses ethical issues in the use, design and management of information technology and in the formulation of ethical policies for its regulation in society [3].

HISTORY OF CYBERETHICS

The concepts of cybernetics, combined with digital computers under development at the time, led Weiner to draw some remarkably insightful ethical conclusions about the technology that we now call ICT (Information and Communication Technology). In his 1948 book, Weiner wrote on "Cybernetics: or control and communication in the animal and the machine," and also in his 1950 book on: "The Human Use of Human Beings" [4-6]. In the mid 1960s, Donn Parker of SRI International in Menio Park, California, examined unethical and illegal uses of computers by computer professionals, and said that: "when people enter the computer center they left their ethics at the door." Parker produced books, articles, speeches and workshops that re-launched the field of computer ethics, giving it momentum and importance that continue to grow today [7, 8].

The late 1960s witnessed Joseph Weizenbaum, a computer scientist at MIT in Boston created a computer called ELIZA, which he scripted to provide a crude imitation of "a Rogerian psychotherapist engaged in an initial interview with a patient." He was concerned that "information processing model" of human beings was reinforcing an already growing tendency among scientists, and even the general public, to see humans as mere machines," and with his book that expressed some of these ideas [9]. Computer ethics first came about in the 1970s as

computers were becoming more integrated into homes. As at today, computers are used at homes, in schools, and in most companies. Cyberethics has taken ethics to a new level, due to privacy issues surrounding various businesses. Computer ethics was first coined by Walter Maner, a professor at Bowling Green State University, Ohio, which refers to that field of inquiry dealing with ethical problems aggravated, transformed or created by computer technology [10].

IMPORTANCE OF CYBERETHICS

Ethics is what guides us to tell the truth, keep our promises, or help someone in need – a framework of ethics guiding our lives on a daily basis, helping us make decisions that create positive impacts and steering us away from unjust outcomes. Ethics has to do with integrity, value, moral, principles, honesty, conscience, respect for others, justice, lawfulness, and so on. Ethics helps to guide our behavior to make the best choices that will contribute to the common good of all. As taught by our parents and teachers, the basis of ethics is:"do the right thing" [11].

Ethical practices are very essential for the protection of data and maintaining of trust in the present age of cyber security, as shown in Figure 1. As technology advances, we need to uphold a set of standards when handling sensitive information, because of the potential for data breaches, security threats, and cyber attacks. For these reasons, it becomes essential for practitioners to work ethically. A key pillar of the UK Cyber Security Council is to create and enforce an Ethical Standard, which is done through the Ethics Committee and the creation of the Ethical Declaration and reworked Guiding Principles. These are aimed at safeguarding individuals and businesses from unethical cyber activities [12]. Without these guidelines, there can be serious consequences both legally and financially.

The four big areas of computer ethics are [13]:

1. Computer crime
2. Responsibility for computer failure
3. Protection of computer property, records and software
4. Privacy of the company, workers and customers.

Computer crime is an intellectual, white-collar crime. Some examples of this are the stealing of funds via computers, unauthorized computer entry (where the perpetrator can steal a company's trade secrets and data), and hacking, as shown in Figures 2 and 3.

BE ETHICAL ON INTERNET

When using the internet, we should observe and keep to ethical standards, some of which are:

- Be sensitive to national and local cultures: Internet users should be aware, sensitive, thoughtful, and have an understanding about the differences in the national and local cultures of the netizens they meet online. This will help develop a positive and friendly online environment/space leading to fruitful interactions and dynamic cyber society with unity in diversity.
- Use of email and chatting for communication: The internet is to be used for communicating with family and friends but not to be used for chatting or communicating with strangers and not to forward emails from or to strangers because of the risks involved.
- Do not pretend to be someone else on digital space: It is important that all users of the digital space/internet should adopt trustful and truthful means of interaction and communication to promote a healthy, vibrant, positive cyber space that is conducive for growth and progress. The internet is a global medium used for knowledge sharing, interaction, communication, trade, commerce, education, and entertainment.
- Avoid the use of bad or foul language on public platforms: To be kind and considerate is a basic human value or moral principle we are taught in the physical world, and this also applies to the cyber world too. When interaction online, digital users must never be rude or use foul language while using email communication, chatting, blogging, and on any other social networking, knowing that we operate in a global village with no barrier of local and national cultures, hence the need to be considerate and accommodating.
- Protection of personal information: Digital users must ensure to protect their sensitive personal information and to restrict the sharing of such information as their home address, email address, phone number, photographs, passwords to anybody on public platforms while accessing the internet.
- Carefulness when accessing online content and app downloads: Internet users must be careful of downloading applications, music, software, etc., from the internet due to copyright policy. Copyright is the legal protection for the intellectual property rights of authors of original works and therefore be mindful when copying works of others from the internet, so as not to run afoul of copyright laws, as shown in Figure 4.

Honesty is said to be the underlying principle for all computer use, hence users should follow these rules below [14-16]:

Respect the privacy of others,

- Respect the integrity of the computing systems,
- Always identify the user accurately,
- Respect copyrights and licenses,
- Respect the intellectual property of others,
- Exhibit responsibility, sensible use of computer hardware, software and data.
- Ensure the use of the "Ten Commandments of Computer Ethics" introduced by Ramon C. Barquin.
- Some people have the misconceptions that there are no laws governing the virtual world and that their anonymity will save them from being detected. The laws that govern the internet and you may attract legal liabilities if you perform or engage in any of the following activities [17]:
- Posting or disseminating obscene and indecent content on the internet that could be offensive to a reasonable person,
- Obtaining property or services online by deception,
- Spreading viruses, malicious codes or conducting any hacking activities on other computers,
- Disrespect to the right to privacy and legal issues associated with cyber-bullying in the cyber world,
- Disrespect to other internet users through threats, harassment, stalking, abuse, and
- Gaining unauthorized access to computers, etc.

WHAT IS CYBERCRIME?

Cybercrime is any crime that takes place online or primarily online. Cybercriminals often commit crimes by targeting computer networks or devices, as shown in Figure 5. Cybercrime can range from security breaches to identity theft. Others are "revenge porn," cyber-stalking, harassment, bullying, and child sexual exploitation. Also terrorists collaborate on the internet, moving terrorist activities and crimes into the cyberspace. Protect yourself against cybercrime through [18]:

- Use of a full-service internet security suite: Consider trusted security software like "Norton 360 with LifeLock Select," which provides all-in-one protection for your devices, online privacy, and identity, and helps protect your private and financial information when you go online.
- Make use of strong passwords.
- Keep your software updated.
- Manage your social media settings.
- Strengthen your home network: Make use of strong encryption password as well as a virtual private network (VPN).
- Talk to your children about the network.
- Keep up to date on major security breaches.
- Take measures to help protect yourself against identity theft.
- Know that identity theft can happen anywhere.
- Keep an eye on the kids.
- Know what to do if you become a victim: When you become a victim of a cybercrime, alert the local police, also contact the companies and banks where you know fraud occurred, place fraud alerts and get your credit reports.

Cybercrime can be successfully prevented through the setting up of a multidimensional public-private collaborations between law enforcement organizations, the information technology industry, and financial institutions [19]. The impact of cybercrime on the society is far-reaching and could be devastating. Financial cybercrime can result in significant financial losses for both individuals and businesses, which could lead to bankruptcy and unemployment. Identity theft can result in ruined credit scores, loss of reputation, and legal troubles. Cyberstalking and cyberbullying can result to mental health issues, social isolation, and even suicide. It could as well cripple businesses and institutions, resulting in significant economic damage and disruption of critical services like healthcare cum transportation. Attacks on government institutions can compromise national security which could lead to political instability. As opined by Hary Gunarto, encryption technology can be used to minimize harmful actions on the internet [20, 21].

CYBERCRIME DISRUPTION AND PREVENTION

Cybercrime, also known as "computer crime" is the use of computers and the internet to carry out illegal purposes such as online fraud, identity theft, cyberstalking and hacking, among others.

It has been reported how ten years ago, Microsoft's DCU has honed its strategy of using both unique legal and the company's technical reach to disrupt global cybercrime and state-backed actors. The rise of online scamming and cybercrime being curbed by the governments and the tech industry around the world has been on the scramble for some time now. With the progress on digital defenses, enforcement, and deterrence, the ransomware attacks, business email compromises, and malware infections keep coming. For the past decade, Microsoft's Digital Crimes Unit (DCU) has developed its own strategies, both technical and legal, to investigate scams, take down criminal infrastructure, and block malicious traffic, as shown in Figures 6, 7 and 8. The DCU has been to disrupt a cybercrime called Storm-1152 by Microsoft. A middleman in the criminal ecosystem, Storm-1152, sells software services and tools like identity verification bypass mechanisms to other cybercriminals – which has grown into the number one creator and vendor of fake Microsoft accounts, and has created roughly 750 million scam accounts that the actor has sold for millions of dollars [22].

GLOBAL CONCERN

The working of the Federal Bureau of Investigation (FBI) is with federal counterparts, foreign partners, and the private sector to close the gaps the adversaries look for to exploit intelligence and information networks. In the U. S. these partnerships allow the FBI to defend networks, sanction bad behavior, and take the fight to our adversaries overseas. This team approach is achieved through unique hubs where government, industry, and academia form long-term trusted relationships to combine efforts against cyber threats. Within government, the hub is known as the National Cyber Investigative Joint Task Force (NCIJFT). It is only together that we can achieve safety, security, and confidence in a digitally connected world. The FBI works by developing innovative investigative techniques, using cutting-edge analytic tools, or forging new partnerships, and as well as adapting to meeting new challenges from evolving cyber threat via [23]:

- The Internet Crime Complaint Center (IC3) collects reports of internet crime from the public. The use of such complaints by the IC3's Recovery Asset Team has assisted in freezing hundreds of thousands of dollars for victims of cyber crime.
- The CyWatch is the FBI's 24/7 operations center and watch floor, that provides around-the-clock support to track incidents and communicate with field offices across the country.
- The FBI works closely with our international counterparts to seek justice for victims of malicious cyber activity via cyber assistant legal attaches in embassies across the globe.
- The FBI has specially trained cyber squads in each of our 56 field offices. Who work hand-in-hand with interagency task force partners.
- The rapid-response Cyber Action Team can deploy across the country within hours to quickly respond to major incidents.

CONCLUSION

In our new world of information society with global networks and cyberspace is now creating a wide range or variety of political, social and ethical problems. Due to a whole lot of challenges arising from some basic ethical issues on IT on global networks consist of personal privacy, data access rights, and harmful actions on the internet which have been partially resolved through technological approaches like encryption technique, SSL, digital IDs and computer firewalls. There is also the need for legal laws in all countries which should be incorporated into one global network in collaboration with various governments, educational institutions, public and private individuals to address the ethical issues of cyberspace.

Reference

[1] Cyberethics – Wikipedia, http://www.en.m.wikipedia.org/cyberethics

[2] Tavan, H. T., "Cyberethics," In: Runehov, A. L. C., Oviedo, L. (eds.), Encyclopedia of Sciences and Religions, 2013, Springer, Dordrecht, pp. 565-570.

[3] Eric Conrad, Joshua Feldman, "Computer ethics – an overview," 2017, http://www.sciencedirect.com/computer-ethics

[4] Weiner Norbert, "*Cybernetics: Or Control and Communication in the Animal and the Machine*," 1948, Paris, (Hermann & Cie) & Camb. Mass. (MIT Press).

[5] Weiner Norbert, "The Human Use of Human Beings: Cybernetics and Society," Houghton Mifflin, 1950. (Second Edition Revised, Doubleday Anchor, 1954.)

[6] Bynum, Terrell, "Computer and Information Ethics," The Stanford Encyclopedia of Philosophy {Summer 2018 Edition), Edward N. Zalta (ed.), URL=https://plato.stanford.edu/achives/sum2018/entries/ethics-computer/

[7] Parker Donn, "Rules of Ethics in Information Processing," Communications of the ACM, 1968, vol. 11, 198-201.

[8] Parker Donn, "*Ethical Conflicts in Computer Science and Technology*," 1979, AFIPS Press.

[9] Weizenbaum Joseph, "Computer Power and Human Reason: From Judgment to Calculation," 1976, Freeman.

[10] Maner Walter, "*Starter Kit in Computer Ethics*," 1980, Helvetia Press (published in cooperation with the National Information and Resource Center for Teaching Philosophy).

[11] Andy Schmitz, "Business Ethics: The Power of Doing the Right Thing," December 29, 2012, http://www.2021books.lardbucket.org/business-ethics-power-of-doing-the-right-thing

[12] UK Cyber Security Council, "Why do we need ethics in cyber?" March 2023, http://www.ukcybersecuritycouncil.org.uk/why-do-we-need-ethics-in-cyber?

[13] Lou Berzai, "Ethical Problems in Computing," February 12, 2019, http://www.comptia.org/ethical-problems-in-computing

[14] Barquin Ramon C., "In pursuit of 'Ten Commandments' for Computer Ethics," May 7, 1992, Computer Ethics Institute. Retrieved 2013-08-17, http://www.en.m.wikipedia.org/ten-commadments-of-computer-ethics

[15] "CSE Ethical Use of Computers Policy," http://www.engineering.buffalo.edu/cse-ethical--use-of-computers-policy

[16] The case for internet ethics and integrity, http://www.presence.global/the-case-for-internet

[17] Information Security & Internet Services, "Cyber Ethics – GovHK," http://www.gov.hk/cyber-ethics

[18] Alison Grace Johnson, "11 ways to help protect yourself against cybercrime," August 15, 2020, http://www.us.norton.com/11-ways-to-help-protect-yourself

[19] "Cybercrime causes and measures to prevent it," 6 December 2022, http://www.geeksforgeeks.org/cybercrime-causes-and-measures

[20] Laljan Basha Shaik, "The dark side of the internet: Understanding cybercrime and its impact on society," April 10, 2023, http://www.linkedin.com/pulse/dark-side-of-the-internet

[21] Hary Gunarto, "Ethical Issues in Cyberspace and IT Society," http://www.apu.ac.jp/~gunarto/ethical-issues

[22] Lily Hay Newman, "Microsoft's digital crime unit goes deep on how it disrupts cybercrime," Security, December 14, 2023, http://www.wired.com/microsoft's-digital-crime

[23] "Cyber Crime – FBI," http://www.fbi.gov/investigate/cyber-crime

ABOUT AUTHORS

Paul A. Adekunte holds a Masters degree in Crime Management and Prevention from Bayero University, Kano and a Bachelor degree in Zoology from the Ahmadu Bello University, Zaria, Nigeria. He is a seasoned lecturer, trainer and consultant in security matters, human and management/public relations expert.

Matthew N. O. Sadiku is a Professor Emeritus in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interests include computational electromagnetics and computer networks. He is a fellow of IEEE.

Janet O. Sadiku holds Bachelor degree in Nursing Science in 1980 at the University of Ife, now known as Obafemi Awolowo University, Nigeria and Master's degree from Juliana King University, Houston, TX in December 2022. She has worked as a nurse, educator, and church minister in Nigeria, United Kingdom, Canada, and United States. She is a co-author of some papers and books.

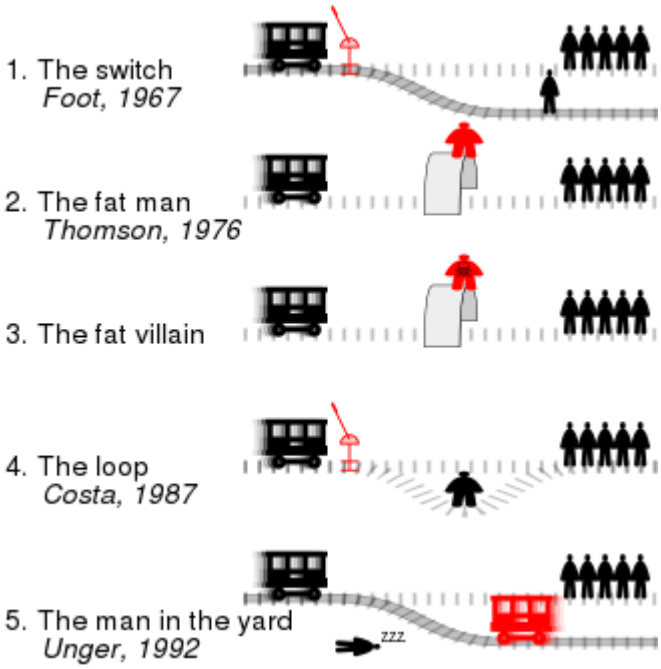


Figure 1 Ethics - Wikipedia

Source:
https://www.google.com/search?q=images+on+cyber+ethics+by+wikipedia&sca_esv=593744898&tbm=isch&sxsrf=AM9HkKk-hl7Db7KR3alFl5BiKSDp_qgzgQ:1703589865481&source=lnms&sa=X&ved=2ahUKEwis_Jjm_qyDAxWSTkEAHZOXBMMQ_AUoAXoECAUQAw&biw=1366&bih=580&dpr=1#imgrc=TSsAdC

Figure 2: Hacker - Wikipedia

Source:
https://www.google.com/search?q=cyber+crime+images+by+wikipedia&tbm=isch&ved=2ahUKEwitmvGxoaeDAxXvQKQEHacjAdwQ2-cCegQIABAA&oq=cyber+crime+images+by+wikipedia&gs_lcp=CgNpbWcQDDoECCMQJzoFCAAQgAQ6BggAEAcQHjoECAAQHjoGCAAQBRAeOgYIABAIEB5Q7wpYrE9gpn9oAHAAeACAAcQIiAHPJpIBDDItMTAuMi42LTEuMZgBAKABAaoBC2d3cy13aXotaW1nwAEB&sclient=img&ei=4LaHZa2qI--BkdUPp8eE4A0&bih=580&biw=1349&hl=en#imgrc=GJ34z3cY9RJjWM

Figure 3: Cyberattack - Wikipedia

Source:
https://www.google.com/search?q=cybercrime+destruction+by+wikipedia&sca_esv=593356401&tbm=isch&sxsrf=AM9HkKnKS2iWUMtLgHbhU_UqCEZjgWoqbA:1703392327702&source=lnms&sa=X&ved=2ahUKEwim-Ov0nqeDAxWBXEEAHao4C30Q_AUoAXoECAQQAw&cshid=1703392328219078&biw=1366&bih=625&dpr=1#imgrc=jX2VXNyMQxyGsM

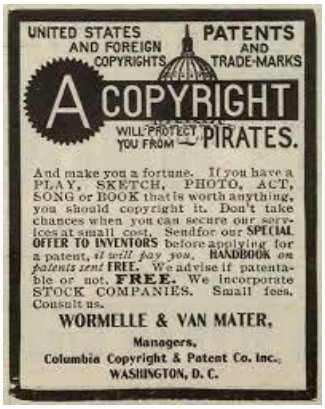


Figure 4: Copyright infringement - Wikipedia

Source:
https://www.google.com/search?q=cybercrime+prevention+by+wikipedia&tbm=isch&ved=2ahUKEwiY9-i5saWDAxXMfqQEHYYNCbIQ2-cCegQIABAA&oq=cybercrime+prevention+by+wikipedia&gs_lcp=CgNpbWcQDFAAWABgAGgAcAB4AIABAIgBAJIBAJgBAKoBC2d3cy13aXotaW1n&sclient=img&ei=SLuGZZizK8z9kdUPhpukkAs&bih=580&biw=1366

Figure 5: Cybercrime - Wikipedia

Source:
https://www.google.com/search?q=cybercrime+prevention+by+wikipedia&tbm=isch&ved=2ahUKEwiPs4-CtKWDAxXPnCcCHX9YAEgQ2-cCegQIABAA&oq=cybercrime+prevention+by+wikipedia&gs_lcp=CgNpbWcQDFAAWABgAGgAcAB4AIABAIgBAJIBAJgBAKoBC2d3cy13aXotaW1n&sclient=img&ei=-b2GZc_SDM-5nsEP_7CBwAQ&bih=580&biw=1366#imgrc=v7i3Hvmmi2R7ZM

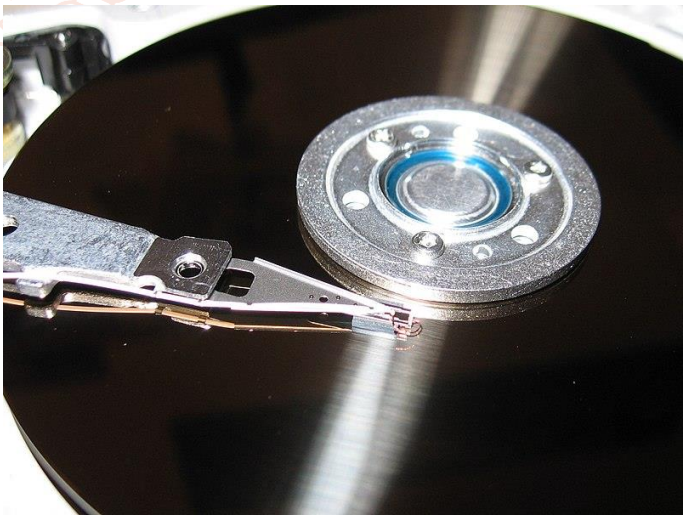


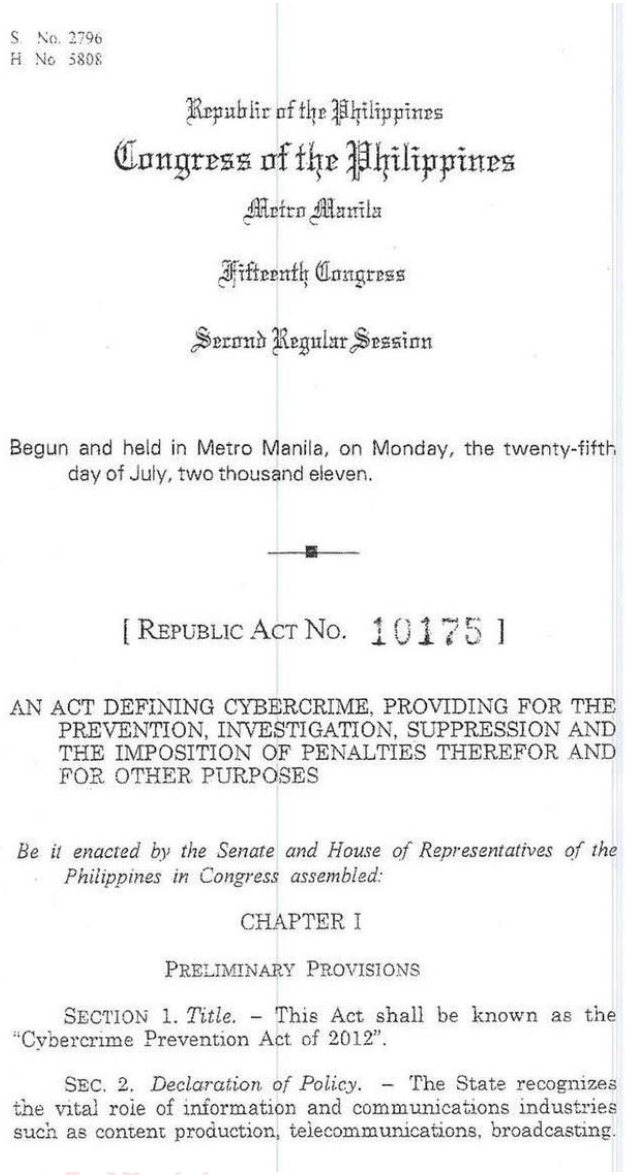
Figure 6: Digital Forensics – Wikipedia

Source:
https://www.google.com/search?q=cyber+crime+images+by+wikipedia&tbm=isch&ved=2ahUKEwitmvGxoaeDAxXvQKQEHacjAdwQ2-cCegQIABAA&oq=cyber+crime+images+by+wikipedia&gs_lcp=CgNpbWcQDDoECCMQJzoFCAAQgAQ6BggAEAcQHjoECAAQHjoGCAAQBRAeOgYIABAIEB5Q7wpYrE9gpn9oAHAAeACAAcQIiAHPJ

pIBDDItMTAuMi42LTEuMZgBAKABAaoBC2d3cy13aXotaW1nwAEB&sclient=img&ei=4LaHZa2qI--BkdUPp8eE4A0&bih=580&biw=1349&hl=en#imgrc=7DSdWwU12mmvMM

Figure 7: Computer security - Wikipedia

Source:
https://www.google.com/search?q=cybercrime+prevention+by+wikipedia&tbm=isch&ved=2ahUKEwiPs4-CtKWDAxXPnCcCHX9YAEgQ2-cCegQIABAA&oq=cybercrime+prevention+by+wikipedia&gs_lcp=CgNpbWcQDFAAWABgAGgAcAB4AIABAIgBAJIBAJgBAKoBC2d3cy13aXotaW1n&sclient=img&ei=-b2GZc_SDM-5nsEP_7CBwAQ&bih=580&biw=1366#imgrc=SjDuULR0ADgRLM



S. No. 2796
H. No. 5808

Republic of the Philippines
Congress of the Philippines
Metro Manila

Fifteenth Congress

Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

[REPUBLIC ACT NO. 10175]

AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I

PRELIMINARY PROVISIONS

SECTION 1. *Title.* – This Act shall be known as the "Cybercrime Prevention Act of 2012".

SEC. 2. *Declaration of Policy.* – The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting.

Figure 8: Cybercrime prevention Act of 2021 - Wikipedia

Source:
https://www.google.com/search?q=cybercrime+prevention+by+wikipedia&tbm=isch&ved=2ahUKEwiPs4-CtKWDAxXPnCcCHX9YAEgQ2-cCegQIABAA&oq=cybercrime+prevention+by+wikipedia&gs_lcp=CgNpbWcQDFAAWABgAGgAcAB4AIABAIgBAJIBAJgBAKoBC2d3cy13aXotaW1n&sclient=img&ei=-b2GZc_SDM-5nsEP_7CBwAQ&bih=580&biw=1366#imgrc=kBlKjB-17RopOM