Ethics and Morals in Cyber Crime: The Concept of Perception Versus Punishment

Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

Dylan Anderson

April 2nd, 2023

Abstract

This interdisciplinary paper examines and discusses the ethical and moral implications of cyber crimes and those who commit them. This paper also seeks to view the current punishments towards cyber crimes compared to how they are viewed by the general public. Cyber crimes and cyberspace are still in their basic stages of infancy and have yet to be fully researched and understood in our current legislative and judicial view. Because of this infancy and lack of understanding of cyberspace and cyber crimes, it is criminal in itself to not view this topic in greater depth. The nature of cyber crimes and crimes require the viewer to also review these crimes and their perpetrators with multiple perspectives in mind to have the most accurate and unbiased view. These disciplines, from a wide range of scholarly articles, studies, and journals review how society, our own human nature, and the United States government shapes and views these cybercriminals who commit these crimes.

Keywords: Ethics, Morality, Cyber crime, Cybersphere, Sociology, Behavioral Sciences, Government, Perception versus Punishment

Ethics and Morals in Cyber Crime: The Concept of Perception Versus Punishment

I've studied cybersecurity both in and out of school for the past eight years. All throughout this time, I had subconsciously determined that cyber crimes are as black and white as normal crimes are and had never really put any extensive thoughts into the reasons these cybercriminals commit these acts. This had drastically changed when I heard from a one off source of the massive amounts of cyber crimes being committed and their perpetrators, which I had to look into myself. Which eventually led me to the realization of the massive amounts of crimes touted as cyber crimes, and their perpetrators. After reading a few of these cases, I learned of the absolute archaic setup of how the United States views and punishes cybercriminals, when the cybersphere is so drastically different from conventional criminal laws. This then finally led me to the creation of the viewpoint of Perception versus Punishment in Cyber crime.

Upon the creation of this viewpoint, I sought out a wide variety of disciplines and viewpoints to further develop my understanding, leading me to select three main disciplines which I want to go over today. The discipline Sociology, which studies how society and one's environment shapes them into who they are; The discipline of Behavioral Sciences, which explores the cognitive processes and common human behaviors; and the discipline of Government, which governs and represents a nation as a whole. These disciplines in conjunction, helped me find out how these cybercriminals are created, how and why they act, and why these cyber crimes are so much harder to punish accurately than conventional crimes.

It is extremely important to view ethics, morals, and crime from a wide variety of different viewpoints. This is one of the main reasons for juries of common citizens being created in the first place, for the most unbiased and reasonable decision towards a crime. There is no doubt this should be the same for cyber crimes and the cybersphere, however, with how early cyber crime research and legislation is in its creation, different methods need to be used to accurately punish these individuals.

One of the biggest factors towards our character is our upbringing, our education and the background around us when growing up. The society we live in shapes us into who we are. Living in a poor state, or ones with a high crime rate tend to create more criminals, and tend to leave the state undeveloped without the possibility to grow. As a consequence to this, the state tends to harbor “negative social and economic” disturbances which strongly affects those living in these less than fortunate communities (Kalu, 2020, p.4). These communities tend to force those living in them into cycles of crime and poverty, which most never escape from, as is the case for conventional crimes. This is not usually the case for cyber crimes however, the societal upbringing of these criminals is far different compared to most other crimes. These cybercriminals tend to come from almost all backgrounds and with most places around the globe having free access to the internet, anyone can commit crimes easier and faster than ever. The internet has allowed these less fortunate and other greedy people the information they need to commit these crimes quickly and with relatively no consequences to speak of. The large economic incentive with little to no consequences of prosecution make these crimes a go-to for honest people who are short on cash and

desperately need the money. However, the ease of access for these crimes also make them a hotspot for scammers, hackers, and other malicious, greedy criminals who only seek to further themselves financially. This therein lies the ethical and moral conundrum, how can these criminals be punished fairly and just? As with all types of crimes, both cyber and regular, “there is no widespread, let alone universal, agreement on what constitutes ethics or morality.”, and in the case of cyber crimes would require “overcoming a set of widely held views about morality itself” (Lucas, 2023). It is paramount that society itself is continually studied as these crimes expand quicker and quicker, as as society further revolves itself around the internet and cybersphere, cyber crimes become ever more rampant.

With one of the key aspects and appeals of the internet being anonymity, the act of complete privacy tends to turn regular citizens into criminals at a moment's notice. Think of it like a 20 dollar bill being found while hiking, there’s no one to see you and no one would ever be able to tell it was you who took it. Most would take this bill a thousand percent of the time. On the internet, this same scenario happens every single day except instead of your normal body you’re wearing a shadowed cloak that prevents anyone from seeing or knowing it’s you. Behavioral Sciences seek to study the mental processes and the science behind human behavior. On the internet, one of the key aspects, anonymity makes one lose a sense of self and allows for dissociation towards crime, making it easier to commit. As stated in *Biology and Cybercrime: Towards a genetic-social, predictive model of cyber violence*, by Tim Owen, “anonymity may allow people to explore their identities, but it also may ‘allow’ them to act without fear of being

held to account for their behaviour in a realm where responsibilities, norms and social restrictions may not apply." (Owen, 1970, p.35). This is one of the main reasons why cyber crimes are becoming so rampant as the years go on, with most places having accessible, free internet almost anyone can commit a crime on anyone anywhere in the globe. Most honest citizens are given a way out of their moral obligations and use this anonymity to commit acts they would never commit in normal circumstances. This therein leads to almost anyone from any background being a potential suspect for a cyber crime, leading for detection of an origin or motive to become almost impossible. Now don't get me wrong, I am not advocating for the removal of privacy from the internet, as anonymity and privacy are not the same thing. As anonymity involves the "desire to hide the identity of the perpetrator of actions that may have grave and harmful public consequences," while privacy on the other hand is a "demand that the public not interfere in an individual's thoughts or actions that have no practical public consequences or significance whatsoever." (Lucas, 2023). Privacy can exist without anonymity, and as anonymity is removed more and more often, the amount of common cybercriminals will decrease as time goes on. With the lack of anonymity, further prosecuting these cybercriminals becomes easier as there is less justification for the common citizen to commit crimes, leading to narrower ethical views and a less complex verdict.

One of the biggest causes for cyber crimes being committed is the lack of prosecution towards these criminals, as most are rarely ever found or even noticed. With millions of cyber crimes happening on the daily, and the sheer lack of incident

response, reporting, and searching, these crimes become so easy to commit almost anyone would do it at least once. This is mainly due to a lack of government resources for proper detection, but most cyber crimes are so complex that the government cannot accurately predict and find these crimes. However, for the criminals who are caught, the punishments are almost always extensive. The government with its still archaic view of the internet and cyber crimes punishes most of these light offenses like they would regular crimes when most are not worthy of them. Take for example one the most widely contested and lambasted by the public acts, The Computer Fraud Abuse Act. Which held extremely harsh punishments for little crimes, resulting in many who were tried being fined heavily and jailed for extensive periods much to public dismay. One of the main reasons for this act's failure and the cause for so much public outcry was the attacker’s motivation and the attacker’s target having almost no effect on sentencing, leading to many crimes being overly and unfairly punished (Graves, 2023, p.316). Take for example the case of Aaron Swartz, who after releasing private university research documents to open sources in the pursuit of free and global information, was sentenced to around 35 years in federal prison and over a million dollars in fines under the controversial CFFA act. The government prosecutor upon the indictment had stated, “stealing is stealing, whether you use a computer command or a crowbar”. Swartz later committed suicide and became a martyr for open information and backlash against the CFAA act (Amsden, 2020). I want to note the university in question later released all documents to the public. The public has shown time and time again its disdain for criminal punishments which are seen as not worthy of the crime, which therein lies the

ethical debate of perception versus punishment. I believe the unbiased public's reaction towards a crime should be an intense motivator for the actual punishment of the crime, which the United States has begun to slowly agree with over time with many amendments added to CFAA and multiple other acts which have lessened the punishments towards small scale crimes, and those with proper motivation, while rightly increasing punishment on specific cyber crimes done by malicious individuals. Take for example the 2008 Information Technology Amendment Act which among many other punishments, states "severe punishment for various cyber crimes including Cyber Terrorism." (IEEE, 2023, p.2). The government has begun strides in the right direction, however it is tantamount to making the punishment fit the crime, as ethics and morals in the cybersphere are far more complex than those in normal society.

While I will not go too in depth, I wanted to mention other subdisciplines I had considered using as they all hold common ground between the main three I've chosen. Education, as education is a main supplement to commit cyber crimes, I believe it falls inside sociology and almost anyone with access to the internet can learn about the ways to commit these crimes. Technology, as technology expands the avenues for cyber crimes to be committed increase, take for example newly developed ai, which can be used for scams or program creations to hack networks, I believe however this discipline didn't have enough meat compared to the other three. These disciplines along with sociology, behavioral sciences, and government all share the common goal of understanding how and why these cybercriminals commit these cyber crimes. Sociology shares social upbringing and interactions to understand how an individual is pressured

to commit these crimes mostly due to financial incentives. These backgrounds from almost anywhere with easy accessibility for anyone from any economic background to the internet allow anyone to have the tools to learn and commit these crimes. Behavioral sciences combine with this understanding to give the motivators for cybercriminals, most commonly being anonymity and lack of prosecution. With anyone being able to access the internet from anywhere to interact with anyone, along with a veil of anonymity, cyber attacks and crimes become commonplace. This also has the unintended negative consequence of making most cyber crimes hard to track. Combine this with growing technology like encryption and identity masking, this process becomes tremendously more difficult. These two disciplines and subdisciplines all then combine to the main discipline of government and the judicial system. This main governing body of the United States represents the public as a whole and such should fairly punish these cybercriminals. Despite this, the government has held an archaic view of cyber crime over the past 20 years with widely contested laws like the CFAA which heavily punished those who committed cyber crimes without much public intervention or effect. One of the main pitfalls of the CFAA spoken earlier was the lack of attacker motivation having an effect on the sentencing of a perpetrator, which had removed the main motivator for most cyber crimes and to make cyber crimes uniform, which is not possible. This then led to the impossibility of the introduction of ethics and morals towards cyber crimes and cybercriminals, treating them as guilty before innocent. However, the public disdain and backlash towards the CFAA over the years has turned this system into a better, while yet flawed view towards understanding the complex

ethical and moral battle towards cyber crimes. This all combined together has led to the creation of the concept of Perception versus Punishment, the process of having the punishment fit how it is widely viewed by the public and motivation, rather than by written down laws. It is again important to note that understanding the ethics and morals towards cyber crimes and the cybersphere in general is an extremely monumental task which requires an overcoming set of widely held views about morality itself, which the public and country has begun to slowly understand and shift towards (Lucas, 2023). As this shift begins to happen, it is important to combine all different perspectives from different cultures and beliefs to accurately gain a deep understanding of the crime being committed, the perpetrator, and their motivations, to accurately perform an unbiased, ethical, and moral view.

These disciplines led to the conclusion of ethics and morals in cyber crime being far more complex than regular crimes. These crimes which are commonplace due accessibility, anonymity, and lack of prosecution have led almost anyone anywhere to be a potential cybercriminal. While societal upbringings cannot be changed immediately and would be extremely difficult to fix, a few other fixes such as the reduction of anonymity and better incident responses towards cyber crimes would allow for more cybercriminals to be found and for common citizens to become far less likely to commit cyber crimes. Another fix which may possibly help would be specific cyber courts, much like civil and criminal courts are done now, as cyber crimes hold a wider scope than crimes with widely different motivations. I cannot stress enough the punishment must fit how the crime is viewed, as ethics and morals in cyber crime are extremely complex. It

is extremely important to understand the motivation of the crime and to accurately give an unbiased view for the best possible scenario.

References

Upadhyaya, R., & Jain, A. (n.d.). *Cyber Ethics and Cyber Crime: A deep dwelved study into ... - IEEE xplore*. Retrieved March 20, 2023, from https://ieeexplore.ieee.org/abstract/document/7813706/

Graves, J., Acquisti, A., & Anderson, R. (n.d.). *Perception Versus Punishment in Cybercrime.* Redirecting... Retrieved March 20, 2023, from https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals%2Fjclc109&id=330&men_tab=srchresults

Lucas, G. (n.d.). *Lucas, G. (n.d.). Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford Academic . Retrieved March 20, 2023, from https://academic.oup.com/book/4922?login=true

Kalu, C. O., Chidi-Kalu, E. I., Okidi, I. A. A., & Usiedo, B. A. (n.d.). *Issues on Information Systems, ICTS, Cyber-Crrimes, Cyber Security, Cyber Ethics, and National Security in Nigeria: Librarians' research*. DigitalCommons@University of Nebraska - Lincoln. Retrieved March 20, 2023, from https://digitalcommons.unl.edu/libphilprac/4182/

Owen, T., Noble, W., & Speed, F. C. (1970, January 1). *Biology and Cybercrime: Towards a genetic-social, predictive model of cyber violence*. SpringerLink. Retrieved March 20, 2023, from https://link.springer.com/chapter/10.1007/978-3-319-53856-3_3

Amsden, D. (2020, January 12). *The brilliant life and tragic death of Aaron Swartz*. Rolling Stone. Retrieved April 9, 2023, from https://www.rollingstone.com/culture/culture-news/the-brilliant-life-and-tragic-death-of-aaron-swartz-177191/