International E-Journal of Criminal Sciences

ISSN: 1988-7949 *UPV/EHU Press* *www.ehu.eus/inecs*

Why People May View Online Crimes as Less Criminal: Exploring the Perception of Cybercrime

Majid Sarfi, Morteza Darvishi and Mostafa Zohouri *
Department of Law, University of Tehran, Tehran, Iran

Abstract

Introduction:
Stats reveal an increasing rate of cybercrimes. Data breaches cost businesses an average of $4.35 million in 2022. This qualitative research explores the realm of cybercrime, focusing on adult perceptions and the underlying factors that might motivate engagement in online activities considered illegal or criminal.
Objectives:
The primary aim of the study is to explore how individuals conceptualize online crimes and rationalize their involvement in such activities, including illegal downloads and online bullying. Understanding these perceptions is crucial for addressing the broader implications of cybercrime in society.
Methodology:
The study gathered insights through panel discussions involving master's students from diverse international backgrounds at the University of Tehran. Thematic analysis was employed to dissect and understand the opinions and justifications offered by the participants regarding their views on cybercrime.
Results:
Findings from the discussions reveal a complex tapestry of attitudes towards cybercrime, encompassing various justifications and rationalizations for participation in illegal online activities. These perspectives provide a nuanced understanding of how cybercrimes are perceived by individuals.
Conclusion:
The research contributes significantly to our comprehension of individual attitudes towards cybercrimes. The insights gained are invaluable for the development of targeted educational programs, interventions, and legal frameworks aimed at effectively mitigating and addressing the challenges posed by cybercrime.

Keywords: illegal; criminal tendency; online crime; rationalization.

*Corresponding author: mostafa.zohouri@alumni.ut.ac.ir

1- Introduction

The rise of the Internet and the expansive growth of online environments have ushered in a revolutionary era, offering numerous benefits to our lives. However, alongside these technological advancements, new avenues for criminal activities have emerged. Referred to as cybercrimes, these illegal activities encompass a broad range of actions conducted through the Internet or other digital networks. From the alarming notion of cyber-terrorism (Janczewski & Colarik, 2007) to the spread of fake news (Sabzali, 2022), these newly evolved criminal actions have captured considerable attention and concern. Online crimes include a wide range of activities, such as identity theft, hacking, phishing, cyberstalking, and online fraud. These crimes are often facilitated by the anonymity and global reach of the Internet, making them difficult to detect and prosecute. As a result, online crimes have become a serious concern for individuals, businesses, and governments around the world.

The impact of online crimes on society is significant. They can cause financial losses, damage to reputation and privacy, and emotional distress for the victims. Online crimes can also have broader social and economic implications, such as reducing public trust in online services and undermining the integrity of online transactions (Younes, 2016). In the case of crimes such as bullying or harassing children, the offenses can go unseen by parents and teachers and therefore they can inflict more harm which adds to the severity of their negative impacts (Strauss, 2013). This is particularly concerning because children may not have the necessary skills or resources to protect themselves from online threats. Moreover, online crimes are often interconnected with other forms of criminal activity, such as drug trafficking, human trafficking, and terrorism. The profits from cybercrimes are used to fund these other forms of criminal activity, making it a global threat to security and stability.

Therefore, it is essential to address the issue of online crimes with proper legal systems that define online crimes and their appropriate level of punishment, proper systems to detect crimes and their perpetrators, proper policing systems that can take action against the perpetration of crimes, and finally proper education to discourage people from committing these crimes. While having proper legal systems, detection systems, and policing systems is crucial for combating online crimes, it is important to recognize that such measures alone may not be sufficient. In order to be a more effective citizen (te repeat terminology of Zuboff (2019)), people must also be well-informed about the severity of online crimes and be ethically opposed to committing them.

Despite the increasing prevalence of cybercrime (Monteith et al., 2021), we have surprisingly little understanding of how people perceive online crime compared to crimes in the physical world (Karagiannopoulos et al., 2021). This lack of knowledge is concerning because it could hinder efforts to combat cybercrime. If people do not understand what actions are considered criminal and why, it may be challenging to enforce laws and hold perpetrators accountable. Furthermore, if people do not perceive online crime as serious as physical crimes, they may be more likely to engage in these criminal activities. In this article, we will explore the perception of online crimes, particularly among people, and examine the reasons why they may view these crimes differently from those committed in the physical world. By doing so, we hope

to shed light on the importance of understanding and improving people's perceptions of online crimes and their serious consequences for society and individuals. Based on the above argument the present study seeks to answer the following question: In what ways people may justify doing illegal actions in cyberspace or see cybercrimes as less significant or illegal?

The present study is not focused on producing generalizable statistics but rather aims to explore the ways in which people may justify doing illegal actions in online environments.

2- Definitions and Scope

The definition of online crimes and their types is a complex and evolving issue. While some acts against computer data or systems are universally recognized as cybercrimes, other forms of online criminal activity can be difficult to define and categorize. Examples of online crimes include hacking, phishing, identity theft, cyberbullying, and the distribution of illegal content such as child pornography. However, the scope of online criminal activity is constantly changing and expanding, as new technologies and communication channels emerge. Therefore, it is important to maintain a flexible and adaptable definition of online crimes in order to effectively combat and prevent such activities.

In the context of online crimes, it is important to define what the term "cybercrime" means. According to a review of the evidence by Dr. Mike McGuire and Samantha Dowling, cybercrime can be broadly classified into two categories: cyber-dependent crimes and cyber-enabled crimes. Cyber-dependent crimes are those that can only be committed using a computer or other form of ICT, such as hacking, the spread of viruses and other malicious software, and DDoS attacks. Cyber-enabled crimes, on the other hand, are traditional crimes that are facilitated or increased in scale or reach by the use of computers or ICT. Examples include fraud, theft of personal information, and sexual offending against children (McGuire & Dowling, 2013).

Cyber-enabled crimes can still be committed without the use of ICT. However, the utilization of technology can render these crimes easier to execute and more challenging to identify. Various offenses, including theft and academic plagiarism (Sabbar, Masoumifar & Mohammadi, 2020), can be facilitated through the use of digital devices and the internet. On the other hand, cyber-dependent crimes are entirely reliant on technology and cannot be committed without it. The Computer Misuse Act of 1990 in the UK provides a legal framework for specific offenses associated with cyber-dependent crimes, such as hacking and the creation or distribution of malware (Correia, 2019). However, cyber-enabled crimes are often not as clearly defined in law, and there may be challenges in identifying and prosecuting such offenses. It is important to have a clear understanding of the different types of online crimes in order to develop effective prevention and detection strategies.

Although cybercrime encompasses a wide range of activities, this research will focus on specific categories. The primary reason for this is that the study aims to understand how real-world crimes and cybercrimes might be perceived differently. As such, it is reasonable to select types of crime that have close equivalents in both the physical and

digital realms. For instance, the researchers may investigate whether an interviewee perceives the act of stealing valuable items in the real world differently from taking their digital belongings. Stealing can take many forms in both the real world and cyberspace. In the physical realm, it can range from eating someone's food without their permission to actively emptying their wallet or shoplifting. In cyberspace, stealing can include using someone's Wi-Fi without their permission or illegally copying software applications, among other activities.

Physical violence is exclusive to the real world, while phishing is specific to cyberspace and therefore the present research will not be studying either physical violence or phishing. Instead, it will consider bullying as an example because it can occur both online and in person. It is possible to use broad and general categories and find equivalents in the other realm. For example, one could argue that in rare situations, verbal violence through the internet has become similar to physical violence. However, it is more accurate to categorize verbal violence separately from physical violence, regardless of whether it occurs in person or through online channels. On the other hand, one could argue that phishing is a form of information theft. While this is correct, phishing refers to a specific technique of information theft that does not have a close equivalent in the real world. For a study such as this one, it is reasonable to focus on main categories (e.g., stealing, bullying) without delving into technical details.

In 2023, Routledge's International Handbook of Online Deviance sought to provide practical suggestions for researchers aiming to measure cybercrime and cyber deviance in surveys (Buil-Gil et al., in press). The handbook categorized cybercrimes into three main groups: cyber-dependent crime (including digital piracy, malware, hacking, spam/phishing, DDoS, etc.), cyber-enabled financial crime (including online shopping fraud, online banking fraud, ID fraud, and advance fee fraud), and cyber-enabled personal crime/deviance (including hate crime, hate speech, and online harassment). The present research will roughly base its categorization on the mentioned categories to provide a list of real-world/cyber equivalent crimes, as presented in Table 1.

Table 1 – List of Equivalent Crimes in Cyberspace and the real world

Examples	**Real-World Crime**	**Examples**	**Cybercrime**
- taking food belonging to others from the workplace fridge - shoplifting from a store - Stealing money or valuables from someone's car or home - taking items from a hotel room - stealing office equipment and supplies from work - taking someone's bike or other property without permission - stealing someone's identity to access their financial accounts	**Theft**	- Online shopping fraud - Online banking fraud - Stealing others' digital belongings such as avatars, game accounts, etc. - illegal download of music, art, films, software, etc. - taking control over websites, and social media accounts for financial gain - hacking VPSs and other service resources in order to avoid paying for the services	**Online Theft**
- advance fee fraud - credit card fraud - identity theft	**Fraud**	- online advance fee fraud - online credit card fraud - online identity theft	**Online Fraud**
- residential property damage (home, trees, etc.) - personal property damage (cars, phones, etc.)	**Property Damage**	- hacking aimed at deleting or manipulating data, etc.	**Online Property Damage**
- hate crime - hate speech	**Hate-based Behavior**	- online hate crime - online hate speech	**Online Hate-based Behavior**
- sexual harassment - bullying	**Intimidation and harassment**	- online sexual harassment - cyberbullying	**Online Intimidation and harassment**
- spreading negative information about a person - ridiculing	**Reputation Damage**	- spreading negative information about a person online - online ridiculing	**Online Reputation Damage**

As explained before, the list was made based on the types of harm rather than the techniques used. So if hacking is used to use resources used by others without their permission it is theft but if it is used to damage other people's property it is property damage. Moreover, under cyber-enabled personal crime/deviance, other than hate crime, hate speech, harassment, bullying, and reputation damage was listed. A different study conducted by Bergh and Junger in 2018 has categorized cybercrimes into six distinct types: "online shopping fraud," "online banking/payment fraud," "other cyber fraud (e.g., advanced fee fraud)," "cyber threats/harassment," "malware," and "hacking" (Bergh & Junger, 2018). As argued "hacking" can result in various outcomes, such as damage, theft, and other negative consequences. Therefore, we recommend that the classification be based on the actual results or impacts of the cybercrimes. Additionally, the mentioned classification does not offer a set of comparable online/offline crime lists. Considering this, we propose the following alternative lists.

The list was not designed to be the most detailed list with no overlapping instances but it provides a comprehensive enough list using which the interviewers can remind the interviewee about different aspects of cybercrime and their equivalents in the real world and encourage them to present the research with their thoughts and feelings regarding those aspects and instances.

3- Literature review

3.1- Perceptions of Crimes and Cybercrimes

The fact that people are spending more and more time on the Internet and cyberspace (Martellozzo & Jane, 2017) is taking up larger parts of individuals' lives necessitates higher attention to the acts and potentials of committing crimes in cyberspace and that in turn necessitates higher attention to people's perceptions of and attitudes toward cybercrimes. There is a growing body of knowledge regarding the perception of cybercrimes and cybercrime tendencies among different groups of people. However, there seems to be a shortage of studies in the field.

Some studies have addressed the perception of people, such as police agencies, who are directly engaged in cybercrime. For instance, a study has investigated the perception of cybercrimes among inspectors and line officers (Lee et al., 2021). Similar to the method used in this study, the study draws the attention of the respondents to specific crimes and their equivalents in cyberspace in statements like this: "Stealing £100 from a person's bank account electronically is equivalent to someone pickpocketing £100" or "Harassment online is less serious than traditional harassment" (Lee et al., 2021).

The mentioned research designed its questionnaire statements to quantitatively measure the respondents' perception of cybercrimes vs. real-world crimes, which makes its approach different from this study. The study concluded that the inspectors mostly perceived online and offline stealing as well as online and offline harassment to be equally serious. However, it observed that the inspectors who had training related to cybercrimes perceived cybercrimes to be more frequent and dedicated more time to

responding to them. Other studies have scrutinized the attitudes of other groups or entities dealing with cybercrimes such as the UK courts (Porcedda, 2023), and why cybercrimes might not receive serious enough sentences.

Many of the studies that can be found by searching keywords related to the perception of cybercrimes focus on such perceptions in a way that does not answer the questions asked by this study. For instance, several studies investigate the way people perceive online *criminals*, rather than online crimes. For instance, a study evaluates high school students' perception of "the online pervert" (Murumaa-Mengel, 2015). Another study investigates the perceived seriousness of white-collar crime and people's opinions regarding policies aimed at reducing such crimes (Simpson et al., 2022). Such studies do not focus on how and why people might be more leaning toward committing online crimes because they perceive them as less serious or for other reasons.

In the field of cybercrime, numerous studies have primarily focused on investigating the perception of crimes from the viewpoint of victims, rather than delving into the motivations and actions of the perpetrators (e.g., Brands & Doom, 2022; Brands & Wilsem, 2021). Moreover, researchers have devoted significant attention to studying cybercrime victimization (Karagiannopoulos et al., 2021). Research in this field spans various aspects, such as identifying common personality traits among cybercrime victims (e.g., de Weijer & Rutger Leukfeldt, 2017) and examining the profound impact of cybercrimes on both individuals and corporations (Button, 2021; Smith et al., 2019).

However, despite this extensive focus on victims, there is a noticeable gap in the existing research concerning the study of the motives and behaviors of average citizens who may engage in criminal activities in cyberspace. Specifically, there is a paucity of investigation into the justifications and rationalizations that may prompt individuals to commit cybercrimes, ultimately making such actions seem more accessible and acceptable. It is crucial to address the dearth of research on the motivations and reasons behind cybercriminal behavior.

4- Methodology

Since the source of data for this study is the participants' self-report, panel interviews were chosen as the most appropriate method for data collection. "In the panel interview format, there is interplay not only between interviewers and interviewees, but also – directly or indirectly – between the interviewees themselves" (Clayman & Heritage, 2005): 299). We decided this strategy would help us getting more honest responses since people are more likely to provide honest response when they interact among peers (Pentland, 2010). A total of 20 master's students studying at the University of Tehran participated in the research. They were chosen by a snowball sampling methodology. At least 43 students were offered to participate among which 20 agreed to cooperate. The participants consisted of people aged between 23 to 43 who use the internet frequently, have experience with cybercrime or have knowledge about it, and come from diverse backgrounds in terms of gender, ethnicity, and socioeconomic status.

The interviews were conducted in the form of two panels, each including 8 to 12 students. The majority of students came from three countries: Iran, China, and Russia. Before the interviews, all participants provided informed consent. The discussion sessions took place in a classroom on the university campus and lasted approximately one hour each. The discussions were transcribed and later used for thematic analysis. Thematic analysis was employed to identify patterns and themes in participants' responses.

The discussions were conducted in a semi-structured format, allowing flexibility in exploring each participant's specific perspectives and attitudes. The interview questions were developed based on the research objectives and literature review and covered various instances of illegal actions in the online environment. Participants were asked to explain whether they found these actions illegal or not, whether they would engage in them or not; in case they said yes to this question, we asked why. The panels were managed by a researcher who maintained a neutral attitude throughout. When presenting any of the categories enclosed in Table 1, the researcher provided many examples to provoke deeper thought from the interviewees. For instance, when discussing stealing, examples such as using unregistered and cracked software programs or someone's online sources (internet, VPS, etc.) were mentioned.

The researcher made efforts to avoid judgmental language, using more neutral terms. For instance, when talking about stealing, the researcher did not use the word "stealing" directly. Instead, they asked if the interviewee would engage in actions like using unregistered and cracked software programs or someone's online sources (internet, VPS, etc.). The same approach was taken for other topics as well, such as replacing "bullying" with asking if the interviewee would make fun of someone "when they say ridiculous things." The researcher aimed to maintain consistency throughout the panels for both online and offline crimes.

As a qualitative work with no intention of generalization, there were not very strict measures of validity and reliability. However, consistency could help receive more authentic, detailed, and open perspectives from the interviewees.

4.1- Qualitative vs. Quantitative Considerations

Qualitative studies are not designed to draw generalized conclusions (Gheondea-Eladi, 2014; Ali & Yusof, 2011; Myers, 2000). However, the temptation to draw generalized ideas can distract researchers from their primary focus. This study is not intended to determine whether the general public takes cybercrime more lightly than real-world crime. Such a study would require a standardized questionnaire, careful sampling, and a sufficiently large sample size. Instead, the current qualitative research aims to better understand the reasons and logic behind people's interpretations of cybercrime whenever they take it lightly. To achieve this, researchers should engage in patient, in-depth conversations with interviewees, presenting them with several examples of

cyber and real-world crimes and asking if they would commit them. The task of drawing the aforementioned comparisons will fall to future quantitative works.

5- Results

The thematic analysis of the ideas expressed by the interviewees provided the following list covering various reasons and justifications for engaging in illegal actions.

1. Minimal Impact

Some interviewees believe that using digital materials or services without paying has little to no negative consequences on the providers or the overall system. The perception that cybercrimes have minimal impact stems from a combination of factors. First, the intangible nature of digital materials and services creates a sense of detachment from real-world consequences. Unlike physically stealing a tangible object, where the immediate impact is evident, the consequences of digital piracy or unauthorized use may not be readily apparent to the individual. Moreover, the widespread availability of pirated content and the prevalence of online platforms hosting such materials create an illusion that a single person's actions would not significantly affect the providers or the overall system.

An interviewee mentions:

Bill Gates will not suffer even if people use his products/services without paying (Interviewee XVIII).

The belief that exceptionally wealthy individuals or large corporations would not suffer adverse effects from piracy is often based on a misunderstanding of their financial capabilities. While it is true that large companies might absorb some losses, piracy, and non-payment can still lead to financial repercussions, especially for smaller businesses and individual content creators who heavily rely on the revenue generated from their products or services.

When it comes to other illegal actions such as bullying, the lack of face-to-face communication may contribute to the illusion that the victim does not suffer. In face-to-face interactions, individuals can directly witness the emotional impact of their actions on others. They can see the immediate distress, fear, or sadness on the victim's face, which can evoke empathy or guilt. However, in the context of cyberbullying, the perpetrator is often physically distanced from the consequences of their actions, making it easier for them to emotionally detach from the harm they cause. A similar argument can be made for other illegal actions, such as property damage, identity theft, and so on.

2. Wealth Disparity

The concept of wealth disparity was apparent in the participants' descriptions of their approach to cybercrime, specifically concerning their reluctance to pay for digital materials or services. Interviewees who hold this viewpoint believe that the capacity to afford online content is linked to their socioeconomic status. Those who are financially well-off can easily access and purchase these services without any significant impact on their financial well-being. As a result, they may feel less compelled to pay for these materials themselves.

One aspect of this belief centers around the idea of justification through comparison. Some interviewees may argue that since wealthier individuals are already paying for these services, it somehow legitimizes their own non-payment. They may perceive their actions as a form of balancing out the system, where the financial burden of supporting digital content creators and service providers falls on those with more financial resources.

Moreover, this perception of wealth disparity extends beyond individual users to a national or global level. Some interviewees may view certain countries as economically more privileged than others, leading them to believe that these wealthier nations should shoulder a larger responsibility for financial contributions to the cyberspace ecosystem. In this view, a sense of fairness emerges, where the burden of payment is distributed based on a nation's economic strength.

3. Collective Benefit and Access to Knowledge

In the context of taking cybercrime lightly, some individuals emphasize collective benefit and access to knowledge as justifications for not paying for digital materials or services. According to this perspective, the advantages of making these resources freely available to the public outweigh any negative consequences of non-payment.

These interviewees believe that knowledge and scientific findings should be accessible to all, even if it means using them without proper payment. They argue that withholding scientific discoveries is a greater offense than utilizing them without paying, especially considering the challenges faced by scholars and individuals in poorer countries who may lack access to paid resources. In their view, governments and international organizations should assume the responsibility of financially supporting scientists and scientific institutions to ensure that research findings are accessible to everyone.

Such a stance raises important ethical considerations about the impact of financial barriers on education and research, particularly in less economically privileged regions. The restriction of access to critical information can hinder progress in knowledge dissemination and scientific advancements, perpetuating global inequalities.

To address these concerns, some advocate for the principles of the Open Access movement. This movement seeks to democratize knowledge by promoting unrestricted access to scholarly works, including academic articles and research findings. By adopting sustainable funding models, it becomes possible to strike a balance between supporting content creators and ensuring broader access to their work.

However, the issue of copyright and intellectual property rights remains a complex challenge. While the desire to disseminate knowledge for the greater good is evident, content creators' rights must also be respected. Balancing these interests is crucial in creating an equitable and sustainable system for knowledge sharing.

4. Perceived Low Severity and Social Acceptance

Within the realm of cybercrime, interviewees may perceive a lower severity and higher social acceptance for various offenses such as theft, online hate crime, hate speech, sexual harassment, cyberbullying, spreading negative information about a person, and online shaming:

I think online hate speech is often downplayed. People say things online they would never say in person. They think it's less severe. (Interviewee XII).

Cyberbullying is often seen as less serious than physical bullying. Maybe because there's no physical harm, people think it's not as bad. (Interviewee II).

I would like to be ridiculed online, rather than to see real people around me or in my workplace ridicule me. (Interviewee XV).

This perception stems from the differentiation interviewees make between physical crimes and non-material, digital offenses, considering the latter to be less serious.

Individuals who don't take cybercrimes seriously often believe that because these crimes occur online, they are somewhat removed from actual consequences. In contrast to physical crimes, where the effects are immediately obvious, the outcomes of crimes committed on the internet might not be so clear to those who commit them. This perceived lack of tangible harm might lead interviewees to downplay the severity of their actions.

Furthermore, our analysis revealed that they may feel that society, in general, accepts or normalizes certain online behaviors, contributing to the belief that these actions are less harmful. Social media and digital platforms can sometimes inadvertently encourage behaviors that would be unacceptable in offline settings. The anonymity and distance provided by the digital environment can embolden individuals to engage in negative actions they might not consider in face-to-face interactions.

Moreover, interviewees might view online offenses as distinct from traditional crimes and therefore less culpable. For instance, they may argue that posting offensive content or ridiculing someone online does not directly harm them physically or materially, and hence, it is not as serious as physically harming someone or stealing from them. The lack of a direct, immediate victim might lead to a perception that the harm caused is minimal or inconsequential.

This perception of lower severity and social acceptance across various online offenses, including hate crime, hate speech, sexual harassment, cyberbullying, and spreading negative information, could contribute to a broader nonchalance towards these actions. Addressing these issues requires raising awareness about the real-world consequences of online behavior, promoting empathy and responsible digital citizenship, and developing effective measures to prevent and respond to such cybercrimes.

5. Voluntary Contributions and Free Alternatives

This reasoning proposes that people should provide materials or services for free and request voluntary donations instead of enforcing payment. They may also argue that if there are free versions of the same materials or services available, they should not have to pay for them.

6. Trial Usage

Some people who don't view cybercrime seriously use the idea of "trial usage" to rationalize not paying for digital products and services. They see this trial period as a valid method to evaluate the product's quality and appropriateness before deciding to purchase it . For these interviewees, if a trial version is not available, they feel justified in accessing the full services without payment.

From their perspective, engaging in trial usage allows them to test the product's features and functionality, akin to trying out a physical product before purchasing it. If the trial version is not offered or if it fails to meet their expectations, they may rationalize their non-payment as a form of compensation for their disappointment.

These individuals might have had past experiences where they paid for digital goods or services only to be unsatisfied with the results. As a result, they may find this logic reasonable as a means to protect themselves from potential financial losses due to unsatisfactory purchases.

7. Anonymity and Difficulty in Tracking

Certain individuals who take cybercrimes lightly are motivated by anonymity and perceived difficulty in tracking their online activities. They believe that the digital environment provides them with a sense of safety and security, making it less likely for

them to be identified or apprehended for their actions. This line of reasoning might be particularly prevalent among individuals who prioritize self-preservation over ethical considerations.

The internet offers a level of anonymity that is not easily attainable in the physical world. Users can create pseudonymous accounts or access online platforms without revealing their true identities. This perceived anonymity can embolden individuals to engage in cybercrimes, as they may believe that their actions will not be directly linked to their real-world persona.

Addressing this perspective requires raising awareness about the potential consequences of cybercrimes and the importance of responsible online behavior.

8. International Sanctions

Some interviewees hold the belief that in countries facing international sanctions or economic limitations that restrict access to products and services, individuals are justified in using materials or services without paying for them. They argue that the adverse impact of sanctions and economic constraints on their ability to access essential resources grants them the right to circumvent payment for digital goods or services.

One interviewee said:

They cannot ask me to turn off my computer and go back to the Stone Age and if I want to use my computer, I need to use applications to run it, many of which are not free. Now if I download and use those applications, they consider me a thief, and if I do find a way to transfer money and pay for them, I am even a bigger criminal for bypassing international sanctions imposed on my country. In this situation, I believe that it's the creators of these harsh and impractical sanctions who are actually harming the economy of the developers behind these applications, not regular citizens like me (Interviewee V).

Interviewees who advocate for this viewpoint might perceive it as a form of resistance against perceived unjust international policies that hinder their country's economic development and restrict access to essential resources. They might view their actions as a means of asserting their right to information and knowledge, despite the barriers imposed by external forces. These sentiments can be particularly prevalent in countries like Iran, where a segment of society holds the belief that world powers would spare no effort to harm the country's economy (Sabbar et al., 2023).

6- Discussion

The present study aimed to explore the considerations individuals make when engaging in various types of cybercrime. Conducted in Iran, a country facing unique challenges due to international sanctions, and with some participants from Russia, another nation under similar sanctions, parts of the findings shed light on the impact of limited access to digital products on individuals' ethical and legal perceptions and behaviors. While the results may not be universally applicable, they underscore the significance of socio-economic contexts in influencing digital activities and ethical decision-making.

The respondents' remarks revealed a key determinant in their choice to use unauthorized software or partake in other potentially unethical or illegal digital behaviors—the affordability of digital products relative to their income. This issue extends beyond Iran and affects many countries where the cost of digital products proves prohibitive for certain individuals. Understanding these dynamics highlights the importance of considering broader socio-economic factors in the realm of digital activities and their implications for ethical and legal choices.

The primary objective of this article was not to pass judgment on the acceptability or morality of interviewees' justifications. Instead, it sought to gain insight into their thought processes concerning the use of digital products without proper payment. By delving into their perspectives and rationales, a deeper comprehension of the complexities surrounding cybercrime emerges, providing valuable knowledge about how individuals perceive such activities in the digital sphere.

The practical applications of these results are multifaceted. Where flawed reasoning is identified, these insights can inform educational approaches to address misconceptions and promote a more informed understanding of digital ethics. Educators play a pivotal role in shaping a responsible and law-abiding digital culture by debunking flawed justifications.

Furthermore, when interviewees' reasoning is found (even partly) acceptable or highlights the challenges individuals face in accessing digital materials worldwide, these findings can prompt the exploration of alternative solutions. Policymakers and world leaders can recognize that imposing sanctions on countries and limiting their access to essential materials and services may inadvertently contribute to the justification of cyber-attacks against digital producers. Such insights may trigger discussions and initiatives aimed at reevaluating the effectiveness and potential unintended consequences of international sanctions, fostering more thoughtful and balanced approaches in the future.

Why the Emphasis on Cyber-theft? The findings of this study have revealed a notable emphasis on cybercrimes related to online theft of items and services, such as unauthorized downloading and using copyrighted materials without payment, while other forms of cybercrimes, like identity theft and cyberbullying, seem to receive comparatively less attention. This disparity in attention may raise questions about the factors influencing public perception and attitudes toward different cybercrimes. We propose two potential reasons for this:

1. Underreporting of More Serious Offenses: One possible explanation for the discrepancy in perceived severity could be the reluctance of individuals to confess to engaging in cybercrimes that carry more severe consequences. Cybercrimes like identity theft and cyberbullying can cause substantial harm to victims, often leading to emotional distress, financial loss, and reputational damage. As a result, individuals might be hesitant to admit their involvement in such activities due to fear of legal repercussions, social stigma, or feelings of guilt.

2. Perception of Harmlessness in Simple Cybercrimes: One possible reason for the focus of the research findings on the unauthorized use of digital items or services without payment, could be attributed to how individuals tend to justify these kinds of offenses more easily. This focus on minor online theft might be because people have a higher tendency to perceive these actions as relatively harmless. In today's digital landscape, unauthorized downloading of media, software, or other digital content has become commonplace, with many individuals viewing it as a minor offense that does not directly cause harm to individuals or corporations.

In contrast, more severe cybercrimes might be less frequently discussed or justified in the interviews due to their obvious and tangible harm to victims. It is possible that those who engage in serious cybercrimes are individuals who lack ethical considerations or are more willing to disregard the potential harm caused to others.

Future Implications and Research Directions: To further investigate and address the tendency to take cybercrimes lightly, future studies could adopt alternative research methodologies. For instance, researchers might employ anonymous online surveys to encourage participants to provide more candid responses regarding their involvement in various cybercrimes, thus mitigating the underreporting bias. Further research in this area could greatly benefit from a quantitative survey that quantifies the weight and importance of the identified factors influencing individuals' decisions to engage in unauthorized digital activities. This survey-based approach would allow for a more systematic assessment of the prevalence of each justification and help identify which reasons are more commonly held among different groups or demographics. Additionally, such research could provide valuable insights into the varying degrees of societal acceptance and the perceived severity of these actions across different contexts and regions.

REFERENCES

Ali, A. M., & Yusof, H. (2011). Quality in qualitative studies: The case of validity, reliability and generalizability. *Issues in Social and Environmental Accounting*, *5*(1/2), 25-64.

Brands, J., & Van Doorn, J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior*, 127, 107082. https://doi.org/10.1016/j.chb.2021.107082

Brands, J., & van Wilsem, J. (2021). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology*, 18(2). https://doi.org/10.1177/1477370819839619

Buil-Gil, D., Trajtenberg, N., and Aebi, M.F. (in press). Measuring Cybercrime and Cyberdeviance in Surveys. In *Routledge International Handbook of Online Deviance*. Routledge

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., Wang, V. (2021). Victims of Cybercrime: Understanding the Impact Through Accounts. In: Weulen Kranenbarg, M., Leukfeldt, R. (eds) *Cybercrime in Context*. Crime and Justice in Digital Society, vol I. Springer, Cham. https://doi.org/10.1007/978-3-030-60527-8_9

Clayman S. & Heritage J. (2005). *The news interview : journalists and public figures on the air.* Cambridge University Press.

Correia, S. G. (2019). Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales. *Crime Science*, *8*(1), 1-12. https://doi.org/10.1186/s40163-019-0099-7

Cybercrime and Its Victims. (2017). United Kingdom: Taylor & Francis.

de Weijer, S. and Rutger Leukfeldt, E. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, 20(7), 407-412. http://doi.org/10.1089/cyber.2017.0028

Gheondea-Eladi, A. (2014). Is qualitative research generalizable?. *Jurnalul Practicilor Comunitare Pozitive*, *14*(3), 114-124.

Karagiannopoulos, V., Kirby, A., Oftadeh-Moghadam, S., & Sugiura, L. (2021). Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review*, *43*, 105615. https://doi.org/10.1016/j.clsr.2021.105615

Janczewski, L. J., & Colarik, A. M. (2007). Cyber warfare and cyber terrorism. Cyber Warfare and Cyber Terrorism. https://doi.org/10.4018/978-1-59140-991-5

Lee, J. R., Holt, T. J., Burruss, G. W., & Bossler, A. M. (2021). Examining English and Welsh Detectives' Views of Online Crime. *International Criminal Justice Review*, 31(1), 20–39. https://doi.org/10.1177/1057567719846224

McGuire, M., & Dowling, S. (2013). Cyber Crime: A Review of the Evidence. Research Report 75. Home Office

Myers, M. (2000). Qualitative research and the generalizability question: Standing firm with Proteus. *The qualitative report*, *4*(3/4), 1-9.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports*, *23*, 1-9.

Murumaa-Mengel, M. (2015). Drawing the Threat: A Study on Perceptions of the Online Pervert among Estonian High School Students. *YOUNG*, 23(1), 1–18. https://doi.org/10.1177/1103308814557395

Pentland, A. (2010). *Honest signals: how they shape our world*. MIT press.

Porcedda, M. G. (2023). Sentencing data-driven cybercrime: How data crime with cascading effects is tackled by UK courts. *Computer Law & Security Review*, 48, 105793. https://doi.org/10.1016/j.clsr.2023.105793

Reep-van den Bergh, C.M.M., Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime Sci* **7**, 5. https://doi.org/10.1186/s40163-018-0079-3

Sabbar, S.; Hosseini, R.; Nosrati, S.; Sarfi, T.; Sabzali, M. (2023). Sociopolitical Problems on the Screens of Film Festivals: A Qualitative Content Analysis of Recent Iranian and South Korean Award-Winning Films. *Positif Journal*. 23(6). 56-79.

Sabbar, S.; Masoomifar, A. & Mohammadi, S. (2020). Where We Don't Know How to be Ethical: A Research on Understanding Plagiarism. *Journal of Iranian Cultural Research* 12 (3), 1-27. doi:10.22035/jicr.2019.2243.2747

Sabzali, M.; Sarfi, M.; Zohouri, M.; Sarfi, T.; Darvishi, M. (2022). Fake News and Freedom of Expression: An Iranian Perspective. *Journal of Cyberspace Studies*, 6 (2), 205-218. doi: 10.22059/JCSS.2023.356295.1087

Simpson, S. S., Galvin, M. A., Loughran, T. A., & Cohen, M. A. (2022). Perceptions of White-Collar Crime Seriousness: Unpacking and Translating Attitudes into Policy Preferences. *Journal of Research in Crime and Delinquency*, 0(0). https://doi.org/10.1177/00224278221092094

Smith, K.T., Jones, A., Johnson, L. and Smith, L.M. (2019), "Examination of cybercrime and its effects on corporate stock value", *Journal of Information, Communication and Ethics in Society*, Vol. 17 No. 1, pp. 42-60. https://doi.org/10.1108/JICES-02-2018-0010

Strauss, S. L. (2013). *Sexual harassment and bullying: A guide to keeping kids safe and holding schools accountable*. Rowman & Littlefield.

Younes, M. A. B. (2016). Effects of Cybercrime and Ways to Deal with it. *The International Journal of Engineering and Sciences*, *5*(2), 23-27.

Zuboff, S. (2019). *The age of surveillance capitalism*. Profile Books.