Journal of Islamic Educational Research (JIER)
e-ISSN: 0128-2069

Cybercrime in Contemporary Society: An Islamic Worldview on Its Framework, Motivations, and Consequences

Khalil Al Fazari*, Mohamad Azrien Mohamed Adnan & Tengku Sarina Aini Tengku Kasim*****

Article Information

Received:
29.05.2025

Accepted:
21.06.2025

ABSTRACT

This article examines cybercrime through a threefold lens: its conceptual framework, underlying motivations, and consequences, with an added emphasis on the Islamic worldview. Using a descriptive-analytical method, the study explores how cybercrime encompassing acts like hacking, data theft, and online fraud is driven by diverse motivations, including economic, psychological, social, technological, political, and sexual factors. Beyond conventional analysis, the study incorporates Islamic reflections on these motivations, highlighting ethical and spiritual dimensions often overlooked in secular discourse. The impacts of cybercrime are categorized into six domains: economic, psychological, social, legal, security, and moral-spiritual consequences. From an Islamic perspective, cybercrime erodes moral consciousness *(taqwa)*, promotes unethical behavior, and disrupts societal harmony. The study stresses the need for comprehensive strategies that integrate legal, technological, and ethical measures, including faith-based digital ethics. This approach contributes to a more holistic understanding of cybercrime in contemporary society.

Keywords: Cybercrime, Motivation, Impact, Islamic Worldview, Digital Ethics, Cybersecurity

Citation Information: Al Fazari, K., Mohamed Adnan, M. A., & Tengku Kasim, T. S. A. (2025). Cybercrime in contemporary society: An Islamic Worldview on its framework, motivations and consequences. *Journal of Islamic Educational Research, 11*(1), 46-62.

1. INTRODUCTION

In the midst of the ongoing technological revolution, cybercrime has emerged as one of the most formidable challenges facing individuals and societies today. No longer confined to data breaches or unauthorized system access, cybercrime now extends to psychological coercion and the disruption of social order, rendering it a multidimensional and evolving threat. The gravity of this issue lies in its transnational character and its indiscriminate impact across all segments of society, particularly vulnerable populations such as women and children.

In line with the title of this study, which emphasizes an Islamic worldview, it is crucial to note that Islamic ethical teachings provide a valuable framework for understanding and addressing cybercrime. The principles of justice *('adl),* trust *(amānah)*, and moral accountability *(mas'ūliyyah)* are central to Islamic thought and offer an ethical compass for navigating the complexities of digital misconduct. This study, therefore, integrates these values from the outset to provide a spiritually grounded response to cyber threats.

This study is motivated by a growing concern regarding the widening gap between the rapid evolution of cybercrime and the insufficient scholarly engagement with its psychological and sociological dimensions. As the internet becomes increasingly intertwined with the daily lives of youth and students, the likelihood of exposure to cyber threats such as online extortion and digital harassment has surged. These experiences can result in serious psychological ramifications, including anxiety, depression, and in extreme cases, suicidal tendencies. Compounding the problem is the international nature of these crimes, which complicates efforts in tracing offenders and enforcing legal accountability. Thus, there is a pressing need to explore the root causes that drive individuals to commit cybercrimes and to examine the mechanisms through which these offenses affect their victims, issues that constitute the core focus of this research.

* PhD Candidate at the Department of Islamic History, Civilization and Education, Academy of Islamic Studies, Universiti Malaya, 50603 Kuala Lumpur, Malaysia. E-mail: k.s.alfazari@gmail.com.

** Language Lecturer at the Department of Islamic History, Civilization and Education, Academy of Islamic Studies, Universiti Malaya, 50603 Kuala Lumpur, Malaysia. E-mail: mdazrien@um.edu.my.

*** Associate Professor at the Department of Islamic History, Civilization and Education, Academy of Islamic Studies, Universiti Malaya, 50603 Kuala Lumpur, Malaysia. E-mail: tgsarina@um.edu.my.

This article seeks to offer a multidimensional understanding of cybercrime through three primary lenses. First, it investigates the legal and sociological definitions of cybercrime, highlighting its shifting patterns from technical intrusions to online child exploitation. Second, it delves into the motivations behind cybercriminal behavior, whether driven by economic incentives (e.g., profit), psychological impulses (e.g., thrill-seeking or malice), or social factors (e.g., unemployment or familial breakdown). Third, it examines the consequences of cybercrime, which extend beyond financial loss to include enduring psychological disorders, loss of trust in digital systems, and social alienation.

Methodologically, the study employs a descriptive-analytical approach, drawing on a critical review of existing literature including academic research, international policy documents, and legal frameworks. Various definitions of cybercrime are systematically reviewed to construct a coherent conceptual foundation. The motivations behind cybercrime are classified into four main categories: economic, psychological, social, and technical supported by theoretical models such as Social Learning Theory and Self-Control Theory. The consequences are discussed with reference to specific patterns of criminal activity and victim impact.

Significantly, this study frames cybercrime within the Islamic worldview (*al-ru'yah al-Islamiyyah*), which upholds the sanctity of life, property, and dignity as essential pillars of human welfare (*maqāṣid al-sharī 'ah*). Islam commands moral behavior in all spheres, including digital spaces, and explicitly forbids transgression (*ẓulm*), theft (*sariqah*), and slander (*buhtān*). By embedding Islamic ethical principles into the analysis, this study proposes a spiritually grounded framework that not only interprets cybercrime but also suggests value-based strategies for prevention and response.

From this perspective, cybercrime is not merely a legal or social infraction but also a profound moral violation of the principles of justice (*'adl*), trust (*amānah*), and accountability (*mas'ūliyyah*). The Qur'an firmly denounces fraudulent behavior:

> *"Do not consume one another's wealth unjustly or send it [in bribery] to the authorities so that [they might aid] you to consume a portion of the wealth of others, while you know [it is wrong]."* (Al-Baqarah 2:188)

This verse reflects the Qur'anic condemnation of financial deceit, a common feature of cybercrime. Moreover, Islam holds individuals accountable for their actions—both public and private, online or offline:

> *"Indeed, the hearing, the sight and the heart—about all those [one] will be questioned."* (Al-Isra' 17:36)

Therefore, cybercrime stands in direct opposition to Islamic values such as *taqwā* (God-consciousness) and *iḥsān* (excellence in conduct). By integrating psychological, legal, and Islamic perspectives, this study offers a holistic approach to understanding and addressing the complex and growing phenomenon of cybercrime in the digital age.

2. THE CONCEPT OF CYBERCRIME

Cybercrime is considered a modern and evolving form of crime (Ihlihil, 2023). It represents the misuse of digital networks, platforms, and various forms of social media, arising from the rapid technological advancement and the increasing reliance on digital communication tools in the daily activities of individuals, institutions, and governments alike. Despite the extensive discourse surrounding the concept and forms of cybercrime, scholars have yet to reach a consensus on a unified definition. Their conceptualizations differ based on disciplinary perspectives and the lens through which they examine cybercrime. Some define it based on the nature of the crime, others based on the method used, the technical knowledge involved, or the behavioral patterns (Al-Amarat, 2023).

Cybercrime is widely regarded as one of the most complex social challenges in the information age. Unlike traditional crimes, cybercrimes can span multiple jurisdictions and geographical boundaries, posing serious risks to modern internet-dependent economies (Chinedu et al., 2021).

Etymologically, "cybercrime" is composed of two terms: "crime" and "cyber." The term "crime" refers to any act or omission that violates a criminal law and is subject to penal consequences in the form of punishment or preventive measures (Mukdad, 2019). "Cyber," on the other hand, relates to cyberspace, the digital and virtual environment comprising computer networks, the internet, and information systems (Merriam-Webster, 2025).

Cybercrime has emerged as a contemporary phenomenon that continues to grow with the expansion of the internet across different sectors of society. It is unpredictable in its future trajectory and generally refers to acts carried out with criminal intent, using computers or related technologies to achieve personal benefit or illicit gains (Ulo et al., 2024).

Bahri (2021) defines cybercrime as a type of offense wherein the computer plays a central role in its commission. It constitutes a deviation from established norms in the information society, violating social standards and intending to cause harm to others.

Umeugo (2023) describes cybercrime as a broad category of illegal acts carried out using computer systems and digital technologies, driven by in-depth knowledge of computing systems and cyberspace. The tools used in cybercrime are not limited to desktop computers but also include tablets, smartphones, smart devices, and Internet of Things (IoT) technologies.

According to Al-Damour (2024), cybercrimes encompass any criminal activity conducted through or facilitated by digital devices or modern technologies, either directly or indirectly, to commit a predefined offense—whether targeting individuals, institutions, public, or private assets.

Al-Rubaie (2024) defines cybercrime as any deliberate and premeditated targeting of information systems, infrastructure, digital networks, or information technologies, with the intent to undermine their capacity or functionality. This includes activities such as hacking, infiltration, data leakage, or disruption of operations and services.

Like any other crime, cybercrime comprises fundamental legal elements (Al-Sahafi, 2020), including:

a. The Material Element – the tangible aspect of the crime, which includes:

   Criminal Act: The actual act committed by the offender using digital tools or the internet, such as hacking, online fraud, or malware distribution.
   Criminal Result: The consequence of the act, such as data theft, financial loss, or privacy violation.
   Causal Link: The direct causal relationship between the act and its result—i.e., the crime would not have occurred without the offender's digital actions.

b. The Moral Element – the intent behind the act, comprising

   Knowledge: Awareness that the act is illegal and constitutes a crime.
   Volition: The offender's free will in committing the act, without coercion.
   Criminal Intent: The deliberate aim to achieve unlawful outcomes, such as causing harm or obtaining illegal profits.

In light of the foregoing, cybercrime can be comprehensively defined as:

Any unlawful act or omission committed using computers, smart devices, communication networks, or modern information technologies, with the intent to harm individuals, institutions, or property through hacking, fraud, data theft, privacy violation, or digital system manipulation resulting in the infringement of legally protected rights or interests.

3. CAUSES AND MOTIVATIONS OF CYBERCRIME

Motivation is considered a foundational concept in psychology due to its central role in shaping and integrating personality, as well as its direct influence on guiding human behavior. Nearly every action performed by a living being is driven by a goal to be achieved or a need to be fulfilled. Motivation is a fundamental element in the learning process of different behaviors, as it arises either from an individual's perception of the goal or from the anticipation of a reward for performing a specific action. Motivation can originate internally stemming from within the individual or externally, influenced by environmental stimuli (Wasserman & Wasserman, 2020). In general, motivation is defined as *"an internal state that drives an individual to perform a specific behavior, sustains it, and directs it toward achieving a particular goal"* (Abdel Raouf, 2015). Motivation is commonly divided into two main categories:

i. **Intrinsic Motivation**: This type of motivation originates within the individual, driven by personal interest or internal desire. Individuals engage in activities for the sake of enjoyment, fulfillment, or self-actualization, without the need for external rewards (Ali & Hammouk, 2014; Staller & Kirschke, 2021).

ii. **Extrinsic Motivation**: This refers to motivation prompted by external factors (e.g., material rewards). The execution of behavior depends on the presence of these external incentives, and the behavior typically ceases once the motivating factors are removed or diminished (Staller & Kirschke, 2021).

Motivations influence cybercrime in three primary ways (Ulo et al., 2024):

- **Nature and Type of Crime**: Motivations are a major determinant of the form a cybercrime takes. Common types include romance scams, phishing, inheritance fraud, fake news dissemination, cyber espionage, and pharming. Financial gain is among the leading motives for cybercrimes, particularly in cases like sextortion, where victims are blackmailed for monetary benefit.

- **Victim Selection**: Cybercriminals rely on their motivations to determine suitable targets. The condition of the victim is often central to the crime. For example, a desire to obtain trade secrets or intellectual property may lead to corporate cyber espionage between rival firms.

- **Method of Execution**: All criminal behaviors are rooted in rationales and justifications specific to the offender. Cybercriminals choose their methods of execution based on their underlying motivations. For instance, an offender driven by political motives may resort to sophisticated techniques for conducting cyberattacks.

The motivations behind cybercrime vary depending on the type of offense and the objectives of the perpetrators. These can be categorized into several key domains:

3.1. Economic Causes and Motivations

Money is a predominant driving force behind cybercrime, encompassing a broad spectrum of financially motivated illegal activities such as ransomware attacks, identity theft, email and internet fraud, and attempts to acquire credit card numbers, bank account information, or other payment data (Hizam, 2024). Cybercrime has become a major source of income for many online offenders, with financial incentives prompting individuals and organized groups to engage in such activities.

Cybercrimes offer a seemingly effortless path to quick monetary gain, bypassing the need for conventional work or investment. Methods often include the theft of banking information, credit card fraud, and digital extortion (Ulo et al., 2024).

According to Li (2017), common methods for obtaining financial profit through cybercrime include:

- Selling information without legal authorization.
- Extorting organizations after breaching sensitive data.
- Embezzling funds from employers via electronic payment systems.
- Illegally acquiring proprietary information and selling it to competitors.
- Stealing credit card data for unauthorized purchases.
- Using stolen personal information to impersonate others for financial gain.

It is evident that **economic motivations** are a primary driver of cybercrime, as offenders seek to exploit digital vulnerabilities and weak security infrastructures to achieve unlawful financial gain. This underscores the urgent need to enhance cybersecurity awareness, implement robust protective strategies, and enact strict legislation to curtail the proliferation of these crimes.

3.2. Social, Psychological, and Personal Motivations

Socio-psychological factors play a significant role in explaining why certain individuals resort to committing cybercrimes. These motivations range from the desire for personal challenge and gain to emotional drives such as revenge. Key motives in this category include:

i. Self-Expression and Ego Gratification

Some individuals commit cybercrimes to enhance their sense of self-importance and demonstrate superiority over others. Offenders in this category may experience frustration due to their perceived inability to compete socially in other domains. As a compensatory mechanism, they showcase their technical prowess by breaching information systems. Successfully hacking systems gives them a sense of technical superiority, even if they lack competence or confidence in other social areas (Li, 2017).

ii. Anonymity in Cyberspace

The anonymity provided by social media and digital platforms empowers individuals to engage in cybercrime with greater confidence. Crimes such as hacking, online fraud, and banking scams are facilitated by the reduced risk of identity exposure. Anonymity also encourages cybercriminals to engage in harassment and cyberbullying by creating anonymous accounts to target peers with abusive content. Furthermore, this anonymity can foster the formation of clandestine criminal networks, where like-minded youth collaborate in illegal cyber activities such as drug trafficking, gang recruitment, or planning illicit actions, while minimizing the risk of detection (Ulo et al., 2024).

iii. Thrill and Excitement

Some offenders are driven by a desire for excitement and personal accomplishment. These individuals may hack into complex systems to boast about their skills or to test the strength of security frameworks. Motivated by exhibitionism, they deliberately carry out sophisticated cyberattacks to experience a sense of power and dominance (Bahri, 2021).

iv. Hatred

Cybercrime may also stem from personal hatred toward a specific target. In such cases, the offender might damage or destroy the victim's computer systems, delete or corrupt sensitive information, expose confidential data to harm competitors or adversaries, or deface websites by uploading offensive or defamatory content (Li, 2017).

v. Revenge

Revenge represents an increasingly relevant motive in understanding cybercriminal behavior. It may manifest in various forms, such as blackmail, and is often linked to emotional distress caused by job loss, economic hardship, or interpersonal conflicts. Economic frustration resulting from unemployment can intensify the desire to retaliate through cyber means (Ulo et al., 2024).

vi. Entertainment and Amusement

Entertainment is a major driver behind cybercrime, particularly among novice hackers who seek to explore digital systems and test their technical skills. This may involve breaching friends' or celebrities' accounts out of curiosity or temporarily disrupting websites simply for fun or experimentation often without the intent to cause actual harm (Bahri, 2021).

vii. Self-Defense

In certain contexts, hacking is used as a form of self-defense. For example, in an effort to prevent the illegal copying of their software, two Pakistani brothers embedded the "Brain Virus" in their programs, which subsequently infected the University of Delaware. Their intention was for the virus to target only those who pirated the software, functioning as an automated retaliatory tool. Similarly, members of a religious sect in an Asian country resorted to hacking after their group was labeled a "dangerous cult" and banned by the government. In response, they infiltrated satellite broadcasting systems and replaced official television programs with footage that promoted their version of the "truth" (Li, 2017)

viii. Access to Confidential Information

Some individuals or entities engage in cybercrime with the intent of accessing sensitive or restricted data. This includes corporate or government espionage, theft of scientific research or trade secrets, and hacking of security systems to uncover information that would otherwise be inaccessible through legal means (Bahri, 2021).

ix. Human Negligence

Human error is one of the most significant vulnerabilities exploited by cybercriminals. Despite the presence of advanced security systems, mistakes by users or employees can lead to data breaches or expose individuals and institutions to serious cyberattacks (Rahaman & Hasam, 2021).

x. Collusion and Cooperation

Although psychological, economic, and social factors help explain the rise of cybercrime in modern society, Islamic teachings strongly discourage individuals from yielding to such impulses. The Prophet Muhammad (peace be upon him) said, *"A Muslim*

is the one from whose tongue and hands other Muslims are safe" (Al-Bukhari, n.d., Book 2, Hadith 10). This hadith provides a strong ethical foundation for avoiding any form of harm toward others—whether in the physical world or cyberspace. Islam also emphasizes the importance of moral integrity and self-restraint (*mujahadah al-nafs*), which function as internal mechanisms to deter deviant behavior in a borderless digital environment.

Nevertheless, in reality, many forms of cybercrime today are carried out in a coordinated manner and involve collaboration among individuals or groups with shared interests. These include hacker collectives (*hacktivists*) targeting institutions or governments, insider collusion by employees leaking confidential information, and participation in organized crime networks that exploit the internet for illicit activities such as money laundering, human trafficking, and drug smuggling (Bahri, 2021). Therefore, Islam's emphasis on social responsibility, trustworthiness, and the prohibition of injustice remains highly relevant as a foundational framework for preventing such cybercrimes.

xi. Lack of Awareness About Privacy Risks

Research literature has consistently indicated that user apathy toward privacy concerns stems from a variety of causes. Real threats emerge when users unknowingly grant access to their personal data to unknown third parties. Many individuals remain unaware of how many entities have access to their digital information, enabling third parties to build digital profiles and track online behavior (Rahaman & Hasam, 2021).

It is evident that social, psychological, and personal motivations play a central role in the proliferation of cybercrime. These motivations range from the pursuit of challenge and revenge to desires for control, entertainment, or exploration. Understanding these motives is essential for developing effective strategies to curb this phenomenon. These strategies may include raising awareness about the dangers of cyberspace, enhancing digital protection measures, and enforcing stricter deterrent laws. Moreover, addressing the psychological and social factors that contribute to cyber-offending can help reduce the prevalence of cybercrime and foster a safer, more stable digital environment.

3.3. Political and Legislative Motivations

i. Lack of Effective Legislation and Regulation

The absence of effective legislation and regulatory frameworks represents a major challenge in combating cybercrime. In many countries, laws related to cybercrime remain either inadequate or outdated, failing to keep pace with rapid technological advancements. This legal gap often allows cybercrimes to go unpunished or to be met with insufficient legal deterrents (Taher, 2024).

ii. Mobilization of Political Movements

Government and defense institutions have long been popular targets for cyber sabotage. For example, in 1982, political groups in France repeatedly attacked computer systems under the pretext that technology served the interests of the societal elite. In 1999, the White House homepage was hacked by political activists protesting government policies. Several countries including Italy, former West Germany, the United States, the United Kingdom, Japan, and Scandinavian nations have experienced similar acts of cyber sabotage through both conventional attacks and modern malware. Political hacking has evolved into a radical movement known as **hacktivism**, in which digital activists launch politically motivated attacks on public websites or email servers (Li, 2017).

iii. Lack of International Cooperation

The absence of sufficient international cooperation in tracking cybercriminals enables offenders to exploit legal loopholes across jurisdictions and evade justice. Furthermore, limited legal awareness among individuals and institutions regarding their digital rights and obligations increases their vulnerability to cyberattacks. This highlights the urgent need to develop stronger legal frameworks and intensify awareness campaigns to promote cybersecurity (Taher, 2024).

Political and legislative factors play a crucial role in the spread of cybercrime. Weak legislation, insufficient international coordination, and the political misuse of cyberattacks all contribute to escalating risks in digital spaces. Addressing these challenges requires enhancing legal infrastructures, updating legislation to reflect the evolving nature of cyber threats, and

fostering global cooperation in prosecuting cybercriminals. Raising legal awareness among individuals and institutions is also vital in building a safer and more resilient digital environment.

3.4. Technological Motivations

Technological challenge is among the most compelling motives driving offenders to commit cyberattacks. Many hackers experience a sense of excitement and accomplishment when they successfully breach high-security systems. In one notable case, a hacker developed a Trojan horse program called IPXSRV, which enabled him to take control of 60,000 computers forming what is known as a botnet, a network of compromised devices remotely controlled via chat services or command and control software. The hacker used this botnet to launch a three-month Distributed Denial of Service (DDoS) attack on a music website before being discovered by law enforcement. Investigations later revealed that the hacker's primary motivation was to test the strength of his Trojan, using the website as a trial target (Li, 2017).

Technical superiority is often cited as a key motivator for hackers, alongside the desire for knowledge acquisition, which pushes individuals to engage in unauthorized cyber activities. A prime example is Kevin Mitnick, one of the world's most well-known hackers, whose core motivation was to gain deeper insights into information systems (Li, 2017).

Several technical factors make computer systems vulnerable to cyberattacks, including:

i. **High Data Storage Capacity in Small Spaces**
Massive amounts of data can now be stored in compact digital spaces, making it easier for criminals to extract, transfer, or manipulate sensitive information both physically and digitally.

ii. **Ease of System Access**
Cybercriminals can bypass advanced security systems using tools such as logic bombs, keyloggers, advanced audio recording devices, fake iris recognition systems, and techniques that circumvent firewalls.

iii. **Complex Operating Systems**
Computer systems operate on millions of lines of code, which are prone to human error and exploitable vulnerabilities that attackers can take advantage of (Rahaman & Hasam, 2021).

iv. **Rapid Technological Advancement**
The fast-paced evolution of technology provides increasingly sophisticated tools such as malware, hacking software, artificial intelligence, cloud computing, and the Internet of Things (IoT) which cybercriminals exploit to conduct attacks. The easy availability of hacking tools and spyware on the internet and dark web has contributed to a rise in cybercrime, making it increasingly difficult for security agencies to keep pace with ever-changing threats.

v. **Increased Reliance on Technology**
Growing dependence on technology in nearly all aspects of daily life has made individuals and institutions more susceptible to cyberattacks. The digitization of education, business, and financial transactions has widened the range of potential targets. Storing sensitive data on digital networks has made them attractive to hackers for theft, blackmail, or exploitation. Moreover, the widespread adoption of smart devices and cloud-based services has created numerous security vulnerabilities, escalating risks to information security (Taher, 2024).

Technological factors significantly contribute to the rise of cybercrime. The allure of technical challenge, the evolution of sophisticated tools, systemic vulnerabilities, and increased digital dependency collectively create a fertile ground for cyber-offending. To address these risks, it is essential to strengthen cybersecurity systems, develop advanced strategies to counter cyber threats, and promote technical literacy among users. Furthermore, collaboration among security agencies, developers, and cybersecurity researchers is indispensable for ensuring a more secure digital future.

3.5. Sexual Motivations

Cybercrimes driven by sexual motives are among the most dangerous forms of online offenses. Al-Ghudayan et al. (2018) noted that sexual motives represent one of the highest-ranking triggers for cybercrime compared to other drivers. Sexual violations committed via information systems span various categories of offenses, with the most heavily prosecuted including (Li, 2017):

i. **The production, possession, and distribution of child pornography**, including the recording, storing, transmitting, or selling of illegal content. For example, in the US case of United States v. Ziegler (2007), the defendant used his workplace computer to view, store, and exchange child pornography. The court addressed not only the criminal act but also the issue of digital privacy in the workplace. Similarly, in the UK case R. v. Kasam (2004), the accused was found in possession of thousands of illicit images and videos, including over 3,200 illegal files stored on a single CD-ROM.

ii. **Online sexual harassment**, conducted via text messages, email, or video calls, often enabled by the anonymity provided by digital platforms.

iii. **Promotion of illegal prostitution**, using information systems such as websites or encrypted applications to facilitate illicit operations.

The researcher asserts that sexually motivated cybercrimes pose severe psychological, social, and moral threats to society. With the widespread use of the internet and social media, these crimes have become more complex and prevalent. Addressing them requires strengthened legislation, intensified law enforcement efforts, and increased public awareness regarding personal protection online. Furthermore, cooperation between government institutions and cybersecurity authorities is essential to detect and counter such crimes effectively and to develop mechanisms for tracking and combating illegal digital behavior.

While psychological, economic, and social motivations explain the rise of cybercrime, Islamic teachings warn against succumbing to such impulses. The Prophet Muhammad (peace be upon him) said, *"A Muslim is the one from whose tongue and hands other Muslims are safe"* (Al-Bukhari, n.d., Book 2, Hadith 10). This hadith underscores the ethical imperative to avoid harming others, whether physically or virtually. Islam encourages believers to uphold integrity and self-restraint *(mujahadah al-nafs),* which can serve as internal mechanisms to resist deviant cyber behavior.

3.6. Islamic Reflections on Cybercrime Motivations

Cybercrime, in its various forms, often stems from motivations rooted in material gain, psychological desires, or social factors. From an Islamic worldview *(al-ru'yah al-Islamiyyah)*, these motivations are not merely behavioral impulses but are seen as manifestations of deeper ethical and spiritual deficiencies. Islam approaches crime whether physical or digital as a violation of the moral and legal boundaries set by Allah *(hudud Allāh)*, and hence, the motivations behind cybercrime are to be critically addressed from a moral-spiritual perspective.

i. Greed and Love for Wealth *(ḥubb al-māl)*:
Many cybercrimes, such as fraud, ransomware attacks, and identity theft, are driven by the desire for quick wealth. Islam warns against the unchecked pursuit of wealth, especially through unlawful *(ḥarām)* means. The Qur'an states: *"And do not consume one another's wealth unjustly or send it [in bribery] to the rulers in order that [they might aid] you to consume a portion of the wealth of others while you know [it is unlawful]"* (Qur'an 2:188). This verse prohibits financial injustice and manipulation, which are core elements of cyber-financial crimes.

ii. **Desire for Power, Control, and Fame *(riya' and 'ujb):***
Hackers may commit cybercrimes out of pride, vanity, or a desire for notoriety. This relates to the Islamic concepts of *'ujb* (self-conceit) and *riya'* (seeking fame or showing off). The Prophet Muhammad (peace be upon him) warned, *"He who shows off, Allah will expose him"* (Sahih Muslim, 2986). Islam advocates humility and discourages any form of behavior that seeks to elevate oneself at the expense of others, including unethical displays of skill or intelligence in cyberspace.

iii. **Lack of Taqwa (God-consciousness):**
Taqwa serves as an internal regulator that prevents Muslims from engaging in sinful behavior, even in private or anonymous settings like the internet. Cybercrimes often thrive in the illusion of invisibility, yet the Qur'an reminds: *"He*

knows the stealthy looks and that which the breasts conceal" (Qur'an 40:19). A believer aware of divine surveillance *(muraqabah)* will refrain from committing harm, online or offline

iv. **Social Pressure and Group Influence *(ṭāʿat al-jamāʿah al-fāsidah)*:**
Some cybercriminals act in groups or online forums that promote deviant behaviors, such as hate speech or cyberbullying. Islam acknowledges the effect of peer influence, as stated by the Prophet: *"A person is on the religion of his close friend, so be careful whom you befriend"* (Abu Dawud, 4833). Cybercrime influenced by such environments indicates a need for Islamic social education *(tarbiyyah)* and companionship *(ṣuḥbah)* that fosters righteousness.

v. **Sexual Deviance and Lust *(shahwah)*:**
Cybercrimes like pornography distribution, online grooming, and sextortion are rooted in unchecked lust. Islam strongly prohibits the spread of indecency and exploitation of others for sexual gratification. *"Indeed, those who like to spread immorality among the believers will have a painful punishment…"* (Qur'an 24:19). Such verses highlight the severe moral implications of cybersexual crimes in Islam.

In conclusion, Islamic teachings provide not only legal prohibitions but also internal safeguards against cybercrime motivations through the cultivation of ethical values, spiritual awareness, and communal responsibility. The emphasis on *taqwā, ḥalāl* earnings, and digital *adab* offers a comprehensive framework to prevent cybercrime from an Islamic perspective.

4. IMPACTS OF CYBERCRIME

Cybercrime encompasses a broad array of illegal activities committed in cyberspace, including hacking, financial fraud, identity theft, ransomware attacks, cyber espionage, and the dissemination of malware. The consequences of these crimes are far-reaching, spanning **economic, social, psychological, legal, and security domains**, underscoring the urgent need for robust cyber protection measures to maintain digital safety and societal stability.

4.1. Economic Impacts

Cybercrime represents one of the most pressing economic challenges for governments, businesses, and individuals, leading to both direct financial losses and broader macroeconomic repercussions. Key economic impacts include:

i. **Loss of investor confidence**: Cyberattacks can damage investors' perceptions of a company's reliability, resulting in a decline in market value. Investors require confidence in a firm's digital security before committing capital. A successful cyberattack can severely undermine this trust, reduce company valuation, and increase borrowing costs while hindering capital acquisition for growth.

ii. **Legal liabilities and financial penalties**: Cyberattacks expose businesses to lawsuits and hefty fines, particularly when sensitive customer data is compromised. Organizations may face class-action litigation, leading to reputational damage and diminished customer loyalty, both of which jeopardize financial goals. Customers expect assurance that their data is protected from breaches and malicious actors.

iii. **Direct financial losses**: Firms face high costs related to incident recovery, and cyber insurance premiums may increase as insurers seek to offset the expenses of responding to cyber incidents (Borwell et al., 2022, p. 937; Lee, 2020, p. 26).

Gañán et al. (2017) classified cybercrime-related economic costs into:

i. **Preparedness costs**: Expenses incurred by individuals or organizations to guard against potential cyber threats.

ii. **Incident costs**: Losses resulting directly from cybercrime events.

iii. **Response costs**: Public and private sector expenditures on investigations, legal action, and the implementation of cybersecurity measures.

Paoli et al. (2018) highlighted the severity of these effects, reporting that 32.7% of Belgian companies experienced unauthorized access to their IT systems, and 10.6% fell victim to cyber espionage. Moreover, 15%–20% of affected firms categorized the damage to internal operations as severe, with ransomware identified as the most destructive form of attack.

Riek et al. (2015) found that fear of cybercrime negatively impacts the use of online banking and e-commerce services. Al-Rifai (2024) emphasized that cybercrime contributes to economic distortion and instability, notably through money laundering, which hinders development efforts.

Das and Nayak (2013) noted that the rise of e-commerce has revealed a "dark side" of online business, marked by the proliferation of cybercrimes. This has altered consumer perceptions of online shopping and caused substantial direct financial losses within the private sector. Businesses incur significant costs to secure their operations, including risk assessments, revised procedures, security software, and infrastructure. For complex or sensitive operations, hiring specialized cybersecurity consultants is often necessary.

Cybercrime poses a substantial and far-reaching economic threat, impacting businesses, individuals, and the broader economy. As cyberattacks increase, so do the direct and indirect financial damages. In addition to economic costs, these crimes erode investor confidence, inflate operational expenses, and increase legal exposure. To mitigate these risks, it is imperative to strengthen cybersecurity investments, adopt effective risk-reduction strategies, and raise awareness across sectors. The escalating scope of cybercrime demands coordinated efforts to protect the digital economy and ensure long-term security and resilience.

4.2. Psychological Impacts

The psychological effects of cybercrime on its victims can be profound. Many victims experience a strong sense of personal responsibility for the crime, coupled with limited understanding of what occurred. This often leads to a state known as *"learned helplessness"*, in which individuals feel that any attempt to protect themselves is futile. Consequently, they may exhibit passive and indifferent behavior. As a result, victims often refrain from seeking professional help or psychological support, which exacerbates their psychological symptoms (Ahe, 2022).

Generally, victims of cybercrime are prone to feelings of anxiety, fear, shame or embarrassment, depressive symptoms, low self-esteem, and other psychological problems. The most significant of these include (Borwell et al., 2022; Ahe, 2022):

i. **Anxiety and fear**: Victims may feel unsafe both online and in the real world. They often fear that the offender still has access to their personal information such as bank account details even after the crime has taken place. Additionally, they worry about becoming victims again, as their initial judgment of the offender was flawed, and they fear making the same mistake in the future.

ii. **Shame and embarrassment**: Victims often blame themselves, believing their poor judgment or lack of caution was the reason they became targets. As a result, they may feel naive or incompetent in navigating the digital environment.

iii. **Depression**: Feelings of helplessness, self-blame, fear, and anxiety about the potential consequences of the crime can contribute to the onset of depressive symptoms. Individuals with pre-existing vulnerabilities to mental illness are particularly at risk, as the trauma of cyber victimization can trigger or exacerbate latent psychological conditions.

iv. **Low self-esteem**: Victims may lose confidence not only in their digital skills but also in their ability to assess others' trustworthiness. This erosion of self-esteem affects both personal and professional aspects of their lives.

From an Islamic spiritual lens, engaging in or being victimized by cybercrimes can disturb the balance *(mīzān)* of the individual's soul *(nafs)*. Feelings of betrayal, fear, and shame may weaken spiritual well-being. Islam offers remedies through practices like *tawbah* (repentance), *du'a* (supplication), and reliance on Allah *(tawakkul),* which can provide emotional healing and a pathway to resilience after cyber victimization.

Research literature emphasizes the severity of these psychological consequences. Palassis et al. (2021) found that cyber hacking constitutes a significant violation of an individual's personal digital space, resulting in anxiety, depression, fear of future harm, distrust in digital environments, and negative emotions tied to the loss of privacy, autonomy, and control. These experiences can lead to shifts in victims' beliefs about themselves, society, and safety. Borwell et al. (2022) similarly noted that cyber victimization has a substantial negative impact on psychological well-being. Ahe (2022) also highlighted that cybercrimes targeting individuals tend to produce more severe psychological consequences than other types of cyber offenses. Moreover, the greater the level of interaction between victim and offender prior to the crime, the more intense the psychological harm.

Cybercrime does not only inflict economic harm it also exerts serious psychological tolls, making it a multidimensional threat to both individuals and communities. Victims frequently suffer from anxiety, fear, depression, and shame, all of which diminish their mental health and overall quality of life. The danger lies in the potential development of learned helplessness and low self-worth, which may prevent victims from seeking help or support. To address these challenges, it is essential to raise awareness about cybersecurity, ensure accessible psychological and social support for victims, and implement effective preventive policies. Such measures can contribute to building a safer and more resilient digital environment for all.

4.3. Social Impacts

Crime is a widespread phenomenon found in every society, and it is an inseparable part of social existence. Cybercrimes are among the most serious threats facing modern societies, as their effects extend to various social dimensions. These crimes impact interpersonal relationships, social stability, and even the mutual trust between citizens and governments. Below is an in-depth analysis of the social impacts of cybercrime:

i. Increase in Crime Rates in Society

Cybercrimes facilitate the overall spread of crime by creating a digital environment where criminal acts can be executed without direct confrontation with victims. These include financial fraud, identity theft, cyber espionage, and extortion, all of which contribute to rising crime rates in society (Mehran, 2024). Contributing factors to this rise include (Abdel Gawad, 2023):

- **Low risk of prosecution:** Cybercriminals face less difficulty being tracked compared to traditional criminals, especially with the use of anonymizing and encryption software.
- **Easy access to criminal tools:** The dark web offers a fertile ground for trading malicious tools and software used in cyberattacks.
- **Temptation of quick gains:** Crimes like financial fraud can yield large profits in a short time, attracting individuals driven by greed.

ii. Destruction of Infrastructure

Digital infrastructure is essential for the operation of institutions, companies, and even governments. Cyberattacks on this infrastructure can have catastrophic consequences, including (Mehran, 2024; Abdel Gawad, 2023):

- **Disruption of essential services:** Attacks on public utilities (e.g., power plants or hospitals) can disrupt daily life and jeopardize public safety.
- **Massive financial losses:** Ransomware attacks, for instance, can cost companies billions as they are forced to pay ransom or rebuild their systems.
- **Impact on national economy:** Targeted attacks on banks and major corporations may cause economic disruptions, affecting jobs and investments.

iii. Threat to Social Values

Cybercrimes go beyond material impacts to undermine the ethical and moral foundations of society. Affected areas include (Abdel Gawad, 2023):

- **Spread of unethical content:** The internet facilitates crimes like online child exploitation and the dissemination of violence and hate, eroding moral values.
- **Encouragement of criminal behavior:** Easy access to fraud and data theft tools may normalize unethical behaviors in digital interactions.
- **Erosion of trust and respect culture:** Cyberbullying, defamation, and misinformation campaigns can create a toxic digital environment, harm social relationships and increasing verbal violence and discrimination.

Das and Nayak (2013) noted that societal anxiety over rising crime rates is not due to the crimes themselves, but the potential disruption they cause. Victims may lose valuable things like safety, peace, money, and property that are essential to fulfilling human needs.

iv. Targeting of Critical Sectors

Cybercrimes also affect vital societal sectors by directly compromising basic infrastructure, the economy, national security, and essential services. These include (Mehran, 2024):

- Targeting critical infrastructure
- Attacks on financial and economic institutions
- Cyber espionage and theft of government data
- Cyberattacks on government agencies
- Information manipulation and fake news dissemination
- Threats to the healthcare sector
- Targeting the education sector

v. Exporting a Crisis of Distrust Among Citizens

One of the most dangerous social impacts of cybercrime is the erosion of trust among individuals. When people fall victim to fraud or are exposed to fake news and misinformation, they begin to lose trust in each other and in official institutions. Key indicators of this trust crisis include (Abdel Gawad, 2023):

- **Fear of digital transactions:** Many people avoid online banking or shopping due to fears of hacking and fraud.
- **Doubt in news and information:** The prevalence of fake news makes it difficult to distinguish truth from falsehood, weakening public awareness and spreading informational chaos.
- **Weakened social bonds:** Crimes like cyber extortion and bullying can destroy social relationships, causing people to hesitate in sharing their lives or expressing opinions online.

Research literature highlights the severity of these social impacts. Abdel Gawad (2023) emphasized that cybercrime negatively affects national security and may manifest in deteriorating security and economic conditions. Al-Damour (2024) observed that cybercrime undermines societal culture by affecting traditions, introducing foreign cultures, weakening family ties, and fostering social chaos.

In the same vein, Mehran (2024) noted that cybercrime and cyberattacks pose a serious threat to the social fabric of nations. These transnational crimes target both infrastructure and the social activities of individuals and communities.

The above analysis clearly shows that cybercrimes are not just fleeting digital offenses, but serious social threats impacting all aspects of life. From infrastructure damage and moral value erosion to the cultivation of a trust crisis, these crimes call for a comprehensive response from both governments and communities. The researcher believes that the solutions go beyond enhancing cybersecurity they also require widespread awareness and digital education to ensure safe and responsible technology use in society.

Cybercrimes exhibit deep social impacts that extend beyond individual harm, threatening the social, economic, and security stability of nations. They increase crime rates, damage infrastructure, threaten societal values, break down social bonds, and deepen crises of trust. Hence, countering cybercrime demands integrated strategies involving digital literacy, robust security policies, and cooperation between citizens and governments to build a safer, more trustworthy digital environment.

4.4. Legal Impacts

Cybercrimes have various legal implications that differ depending on the nature of the crime and the legal policies of each country. These crimes give rise to several legal and judicial challenges, especially due to the cross-border nature of the internet and the international scope of cybercriminal activities. Below are some of the key challenges faced in the investigation and prosecution of cybercrimes (Atrey, 2023):

i. Cross-Border Nature

Cybercrimes can be committed in one country while affecting victims in several others. Determining which country has jurisdiction over a cybercrime case can be complex, especially when cybercriminals operate from regions with weak laws or ineffective law enforcement.

ii. Lack of Unified International Legal Framework

Countries vary in their definitions of cybercrime, laws, and penalties. This lack of consistency hinders coordination and complicates international cooperation in cybercrime investigations and prosecutions.

iii. Difficulty in Identifying Perpetrators

Cybercriminals often use techniques to conceal their identities and locations, such as anonymization services, proxy servers, or operating through compromised systems. This complicates jurisdictional determinations and hinders the identification and apprehension of offenders.

iv. Mutual Legal Assistance

Obtaining evidence and cooperation from foreign judicial authorities can require significant time and effort due to the complexities of mutual legal assistance processes. Different countries have varying laws and procedures for evidence exchange and extradition, leading to delays and complications in cybercrime investigations.

v. Limited Resources and Expertise in Law Enforcement

Investigating cybercrimes requires specialized knowledge and technical expertise, which may not be readily available in all countries. Limited financial and technological resources can hinder the capacity of law enforcement agencies to effectively investigate and prosecute cybercrimes.

vi. Jurisdictional Conflicts

When multiple countries claim jurisdiction over a cybercrime case, legal and diplomatic disputes may arise, further complicating legal proceedings.

From the above, it is evident that cybercrimes pose complex legal challenges that demand multi-level responses. The cross-border nature of these crimes, the absence of harmonized international legal frameworks, and the difficulty in identifying perpetrators necessitate stronger international cooperation, the development of more unified and adaptable legislation, and the provision of adequate resources and technical expertise to law enforcement agencies.

4.5. Security Impacts

Cybercrimes have become among the most dangerous threats to national security, as hostile states or terrorist groups can exploit them to destabilize governments and target critical institutions. The risks posed to national security include (Taher, 2024; Abdel Gawad, 2023):

i. **Cyber Espionage**: Certain states or organizations steal sensitive government data, such as military plans or economic strategies.

ii. **Attacks on Infrastructure**: Cybercrimes can disrupt energy, water, and communication systems, resulting in paralysis of essential services for citizens.

iii. **Manipulation of Public Opinion**: Cyberattacks can spread misinformation or manipulate content through social media, creating social and political divisions within nations.

Research literature highlights the severity of the security impacts of cybercrimes. Al-Damour (2024) noted that cybercrime contributes to the erosion of safety within society, fostering widespread fear and increasing levels of anxiety and unrest among individuals.

From the above, it is clear that cybercrimes pose a grave security threat that demands robust defensive strategies to safeguard national security. Cyber espionage, infrastructure attacks, and information manipulation are key tools used to destabilize countries. Therefore, it is necessary to develop advanced cybersecurity systems, strengthen cooperation among security agencies, and raise public awareness on how to confront these threats.

5. MORAL AND SPIRITUAL IMPACTS FROM AN ISLAMIC PERSPECTIVE

Cybercrime does not only produce economic, legal, or psychological harm it also causes deep moral and spiritual damage to both the perpetrator and the wider community. From an Islamic perspective, these impacts are understood through the framework of **sin *(maʿṣiyah)*, moral corruption *(fasād)*,** and the disruption of **social harmony *(iʿtilāl al-niẓām al-ijtimāʿī)*,** all of which are closely linked to the individual's relationship with God (Allah) and others.

i. Erosion of Taqwa (God-consciousness):

One of the gravest spiritual consequences of cybercrime is the weakening of taqwa, or constant awareness of God's presence. The Qur'an emphasizes that true believers are those who fear committing sin even in secret: *"He knows the stealthy glance of the eyes and what the hearts conceal"* (Qur'an 40:19). When individuals commit crimes online—often believing themselves hidden by digital anonymity they progressively lose their sense of muraqabah (divine surveillance), which is a cornerstone of ethical behavior in Islam (Al-Ghazali, 2011).

ii. Accumulation of Sin and Accountability in the Hereafter:

Islam teaches that every action, including those done in cyberspace, is recorded and will be accounted for in the Hereafter. The Qur'an states: *"So whoever does an atom's weight of good will see it, and whoever does an atom's weight of evil will see it"* (Qur'an 99:7–8). Cybercrimes such as slander, fraud, pornography, or data theft become burdens of sin (ʿawāqib al-dhunūb) that spiritually stain the heart (qalb) and distance one from divine mercy unless sincere repentance is sought.

iii. Corruption of Akhlaq (Islamic Morality)

Cybercrime encourages behavior that is antithetical to the values of akhlaq al-karimah, such as honesty, modesty, trustworthiness, and respect for others' rights. The Prophet Muhammad (peace be upon him) said: *"The best among you are those who have the best character"* (al-Bukhari, 6035). Involvement in deceit, manipulation, or immorality online fosters a hypocritical and selfish character that contradicts the prophetic model of integrity.

iv. Desensitization to Evil *(Tajaṛru' al-maʿṣiyah)*

Regular engagement in cybercrimes can lead to moral numbness. Repetition of sinful acts without immediate worldly consequences often desensitizes individuals to the gravity of their actions. This is known in Islamic thought as *istikhfāf al-maʿṣiyah*—treating sins lightly. The Prophet warned: *"Beware of minor sins, for they gather upon a person until they destroy him"* (Ahmad ibn Hanbal, n.d., vol. 5, p. 331).

v. Damage to the Social Moral Order (al-nizām al-akhlāqī)

The cumulative effect of widespread cybercrime is a breakdown of trust and moral order in society. When deception, dishonesty, and violation of rights become normalized, it undermines ʿadl (justice), amānah (trust), and ukhuwwah (brotherhood) key foundations of an Islamic social system. The moral decay of individuals leads to societal disintegration (Nasr, 2002).

In sum, cybercrime from an Islamic perspective is not just a breach of law but a moral-spiritual transgression that impacts the soul, weakens faith, and threatens the ethical fabric of the ummah. Islam provides both preventive ethics and restorative mechanisms such as repentance *(tawbah),* ethical education *(tarbiyyah),* and communal accountability *(ḥisbah*) to heal the moral damage caused by such acts.

6. CYBERCRIME THROUGH THE LENS OF ISLAM

Within the Islamic worldview, cybercrime is not merely a legal violation—it is a sinful act that undermines the principles of justice *(ʿadl),* trust *(amanah),* and accountability *(mas'uliyyah).* Islam places great emphasis on the sanctity of human dignity, property, and rights, all of which are central to the higher objectives of Islamic law *(maqasid al-shari'ah),* which aim to protect

religion, life, intellect, lineage, and wealth (Kamali, 2008). Therefore, acts such as online fraud, data theft, cyber extortion, defamation, and invasion of digital privacy are in direct contradiction with Islamic teachings.

The Qur'an firmly states: *"O you who have believed, do not consume one another's wealth unjustly..."* (An-Nisa', 4:29). This verse prohibits any form of unlawful appropriation of wealth, including through digital means such as phishing or hacking into bank accounts. Furthermore, the prohibition against deceit and theft is reinforced in another verse: *"And do not consume one another's wealth unjustly or send it [in bribery] to the rulers..."* (Al-Baqarah, 2:188), forming the ethical basis for outlawing financial cybercrimes and digital dishonesty.

In the context of individual responsibility in cyberspace, the Qur'an emphasizes: *"Indeed, the hearing, the sight, and the heart—about all those [one] will be questioned"* (Al-Isra', 17:36). This verse reminds Muslims that every action—including those in the digital world—will be held accountable before God. Thus, concepts such as *hisbah* (moral supervision) and *taqwa* (God-consciousness) are crucial in shaping ethical behavior online.

Prophetic tradition also outlines clear moral guidelines for social interaction, including in cyberspace. The Prophet Muhammad (peace be upon him) said: *"A Muslim is the one from whose tongue and hands other Muslims are safe"* (Sahih al-Bukhari). In the digital era, this "tongue and hands" extends to keyboards and online communication, making actions like cyberbullying, slander, and spreading fake news a violation of Islamic ethical conduct.

Islam also views cybercrime as a betrayal of *amanah* (trust). When a person uses technological skills to exploit or damage systems, it constitutes not only a legal offense but also a breach of social and moral contracts within the Muslim community. Therefore, Islamic education (*tarbiyyah*) must promote *akhlaq al-dijitali* (Islamic digital ethics) as a preventive measure among youth and professionals.

In conclusion, the Islamic perspective on cybercrime emphasizes the integration of legal accountability and spiritual responsibility. Addressing cybercrime is not limited to technical or legal measures, but also requires nurturing God-consciousness, integrity, and ethical awareness. An Islamic solution involves value-based education, spiritual development, and the cultivation of responsible digital citizenship to create an ethical and secure cyber society.

7. CONCLUSION

This study has presented a comprehensive analysis of cybercrime, beginning with its conceptual foundations, followed by an examination of its underlying motivations, and concluding with its multifaceted consequences. The findings underscore the complexity of cybercrime and highlight the urgent need for a multidimensional response that includes legal, ethical, social, and spiritual considerations.

Conceptually, cybercrime refers to the use of digital technologies to commit unlawful acts, including unauthorized system access, data theft, identity fraud, and digital extortion. Although terminologies such as "cybercrime," "electronic crime," and "internet crime" may vary across jurisdictions, they commonly share the essential components of criminal conduct and intent. The dynamic nature of these crimes, coupled with the absence of a universally accepted legal definition, continues to pose challenges for legislators and enforcement bodies at the national and international levels.

The study identified various motivations that drive individuals toward cybercrime, encompassing economic, psychological, social, technological, and political dimensions. Economically, cybercriminals often pursue illicit financial gain through fraud or extortion. Psychologically, some perpetrators are motivated by curiosity, self-validation, or the thrill of overcoming digital barriers, particularly among tech-savvy youth. Socially, cybercrime may emerge as a response to marginalization, familial breakdown, or unemployment. Technological motivations include exploiting system vulnerabilities, while political agendas may drive cyberattacks aimed at destabilizing state institutions or promoting ideological goals.

The consequences of cybercrime are extensive and deeply disruptive. Economically, it results in financial losses, damages to business reputation, and a decline in investor confidence. Psychologically, victims may suffer from trauma, anxiety, and feelings of violation, especially in cases involving cyberstalking or sexual extortion. Socially, these crimes erode interpersonal trust, weaken family ties, and normalize harmful digital behaviors. Legally, the transnational nature of cybercrime complicates the prosecution process and hinders effective cooperation across borders. From a security standpoint, cyberattacks can target critical infrastructure and disseminate disinformation, posing threats to national stability.

Importantly, this study also examined cybercrime through the lens of the Islamic worldview *(al-ru'yah al-Islamiyyah),* which provides a spiritually grounded and morally coherent framework for understanding and addressing such crimes. In Islam, the sanctity of life, property, dignity, and public trust are central values protected under the objectives of Islamic law *(maqasid al-shari'ah)*. Cybercrime, therefore, is not merely a legal transgression but also a moral and spiritual violation. Islam unequivocally prohibits acts such as theft *(sariqah),* slander *(buhtan),* deception *(ghurur),* and injustice *(ẓulm),* whether committed physically or in virtual spaces.

From this perspective, addressing cybercrime must move beyond punitive measures to include the cultivation of ethical consciousness, spiritual accountability, and social responsibility. Islamic education (tarbiyyah) can instill values such as taqwa (God-consciousness), digital amanah (trust), and collective moral obligation *('asabiyyah),* thereby fostering a digitally responsible society. This faith-based approach reinforces the human dimension often neglected in secular strategies and promotes a value-driven digital culture aligned with shari'ah principles.

Future research could build on this conceptual framework by conducting empirical investigations into how Islamic digital ethics can be operationalized in cybersecurity practices. Studies could also explore comparative faith-based approaches to digital conduct, evaluate the effectiveness of Islamic educational interventions in reducing cyber-offending among youth, and analyze case studies that integrate shari'ah principles in national cybersecurity strategies. These directions would further substantiate the conceptual claims presented here and contribute to a richer, interdisciplinary discourse.

In conclusion, the study affirms that countering cybercrime requires a holistic strategy that integrates robust legal mechanisms, digital literacy, international collaboration, and moral-spiritual frameworks. By incorporating the Islamic worldview, stakeholders can develop more ethically grounded and culturally resonant solutions to cyber threats. Ultimately, the goal is to build a secure, just, and morally conscious digital environment that protects individual rights, upholds public trust, and contributes to the sustainable well-being of society.

Contribution Rates of Authors to the Article

Author 1 (Main Author): 60% – Developed the conceptual framework, conducted the literature review, and wrote the core sections of the article.

Author 2: 25% – Contributed to the integration of Islamic perspectives, reviewed the manuscript critically for intellectual content, and is responsible for correspondence during the submission and review process.

Author 3: 15% – Assisted with editing, final proofreading, and referencing.

Support Statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Acknowledgement

Special appreciation is extended to academic colleagues who shared their views on the Islamic ethical implications of cybercrime. Their feedback contributed meaningfully to the shaping of the final manuscript.

Statement of Interest

Authors have no conflict of interest.

REFERENCES

Abd al-Jawwād, N.A.A. (2023). Al-Jarīmah as-Sibrāniyyah wa Ta'thīruhā 'ala al-Amn al-Qawmī al-Miṣrī: Dirāsah Sūsiyū Taḥlīliyyah. *Majallat Kulliyat al-Ādāb, Jāmi'at al-Fayyūm,* 15(1), 2083–2149. Retrieved from https://journals.ekb.eg/article_327238.html

Abdel Raouf, T. (2015). *Mental maps and learning skills*. Cairo: Arab Group for Training and Publishing.

Ahe, L. V. D. (2022). *Mental Wellbeing and Cybercrime (The Psychological Impact of Cybercrime on the Victim)* [Bachelor's thesis, University of Twente]. University of Twente Student Thesis. https://purl.utwente.nl/essays/91014

Ahmad ibn Hanbal. (n.d.). *Musnad Ahmad ibn Hanbal*. Riyadh: Darussalam.

Al-Bukhari, M. I. (n.d.). *Sahih al-Bukhari* (M. M. Khan, Trans.). Riyadh: Darussalam

Al-Damour, A. M. (2024). Cybercrimes and their impact on community security in the United Arab Emirates. *Al-Fikr Al-Shurti (Police Thought Journal),* 33(131), 19–64.Al-Ghadyan, Sulaiman bin Abdul-Razzaq, Khatatbih, Yahya bin Mubarak, & Al-Naimiy, Izz al-Din Abdullah. (2018). Forms of electronic extortion crimes, their motives, and the psychological effects resulting from them from the perspective of teachers, board members, and psychological counselors. *Security Research Journal*, 27(69), 157-227.

Al-Ghazali (2011). *Revival of Religion's Sciences* (M.M. al-Sharif, Trans.). Beirut: Dal al-Kotob al-Ilmiah.

Al-Rubaie, N. M. (2024). Cybercrime and combating mechanisms: A comparative study. *Al-Farabi Journal for Humanities, 1*(3), 73–90.

Al-Sahafi, R. A. A. (2020). Cybercrimes. *Comprehensive Multidisciplinary Electronic Journal,* (24), 1–53.

Al-Amarat, F. M. (2023). The problem of stability and national security in the face of cybercrime. *Al-Markaz al- 'Arabī lil-Buḥūth wa-al-Dirāsāt*, (104), 12–23.

Ali, M. Q & Hammouk, W. S. (2014). *Mental motivation: A new perspective.* De Bono Center for Teaching Thinking.

Atrey, I. (2023). Cybercrime and its legal implications: Analysing the challenges and legal frameworks surrounding cybercrime, including issues related to jurisdiction, privacy, and digital Evidence. *International Journal of Research and Analytical Reviews*, *10*(3), 183-197.

Bahri, S. & Kharmoush, M. (2021). The psychological motives behind cybercrime. *Journal of Studies in the Psychology of Deviance,* 6(1), 36–59.

Borwell, J., Jansen, J., & Stol, W. (2022). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review*, 40(4), 933-954. https://doi.org/10.1177/0894439320983828

Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime detection and prevention efforts in the last decade: an overview of the possibilities of machine learning models. *RIGEO: Review of International Geographical Education,* 11(7). 956-974. Retrieved from https://www.researchgate.net/publication/355668267_Cybercrime_Detection_and_Prevention_Efforts_in_the_Last_Decade_An_Overview_of_the_Possibilities_of_Machine_Learning_Models

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies*, 6(2), 142-153.

Gañán, C. H., Ciere, M., & Van Eeten, M. (2017). Beyond the pretty penny: The economic impact of cybercrime. *Proceedings of the 2017 new security paradigms workshop*, 35-45. https://doi.org/10.1145/3171533.3171535

Hizam, A. (2024). Types of cybercrimes and digital forensic investigation tools: A review. *Al-Andalus Journal,* 19(11), 7–24.

Iḥliḥil, K. (2023). Cybercrime and international efforts to counter it. *International Electronic Journal for Legal Research*, 1(3), 7–47.

Kamali, M. H. (2008). *Shari'ah Law: An Introduction*. Oxford: Oneworld Publications

Lee, C. S. (2020). Toward Mitigating, Minimizing, and Preventing Cybercrimes and Cybersecurity Risks. *International Journal of Cybersecurity Intelligence & Cybercrime*, 3(2), 1-3.

Li, X. (2017). A review of motivations of illegal cyber activities. *Kriminologija & socijalna integracija: časopis za kriminologiju, penologiju i poremećaje u ponašanju, 25*(1), 110-126. https://doi.org/10.31299/ksi.25.1.4

Mehran, A. G. (2024). Social repercussions of cybercrimes on Egyptian national security: Confrontation mechanisms. *Military Academy for Postgraduate and Strategic Studies*, 4, 88–103.

Merriam-webster. (2025). *Cyber*. https://www.merriam-webster.com/dictionary/cyber

Mukdad, A. (2019). On the nature of crime. *Jeel Journal of Humanities and Social Sciences,* 59, 123–135.

Nasr, S. H. (2002). *The Heart of Islam: Enduring Values for Humanity*. New York: HarperCollins

Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An exploration of the psychological ımpact of hacking victimization. *SAGE Open,* 11(4), 1-12.

Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change*, 70, 397-420.

R. v. Kasam, [2004] ONCJ 136 No. 3297.

Rahaman, K. H., & Hasam, M. A. (2021). A Social Review on Nature & Reason of Cyber-Crime and the Laws Regarding Prevention in Bangladesh. *International Journal of Research and Innovation in Social Science*, 5(07), 171-178.

Riek, M., Bohme, R., & Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, 13(2), 261-273.

Staller, T., & Kirschke, C. (2021). *Personality Assessment with ID37: Motivation and the Ability to Self-direct*. Springer Nature.

Taher, H. M. (2024). Cybercrimes in the metaverse: Toward effective legal strategies. *The Legal Journal,* 22(2), 691–720.

Ulo, E., Obire, M. O., Akpumuvie, C. E., & Ogbeide, H. E. (2024). Motivational Analysis Behind Cyber Criminal Behaviour in Nigeria. *European Journal of Arts, Humanities and Social Sciences*, 1(5), 61-71.

Umeugo, W. (2023). Cybercrime awareness on social media: A comparison study. *International Journal of Network Security & Its Applications*, 15(2), 23-35.

United States v. Ziegler [2007] 474 F.3d 1184**.**

Wasserman, T., & Wasserman, L. (2020). *Motivation, effort, and the neural network model*. Heidelberg: Springer.