ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 04 No. 02. October-December 2025.Page# 2736-2747
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems

Responsibilities of Concerned Institutions to Overcome Cybercrime

Hafiz Muhammad Jamil Ur Rehman
Ph.D Islamic studies scholar The University of Faisalabad
Registration Number: 2023-Ph.D-IS-002
Email: jamiljee1@gmail.com
Professor Dr. Matloob Ahmad. (Corresponding Author)
Dean Faculty of Arts and Social Sciences The University of Faisalabad.
Email: dean.is@tuf.edu.com

Abstract:
Cybercrime has emerged as one of the most complex challenges confronting modern states, particularly in developing countries such as Pakistan, where rapid digitalization has not been matched with adequate institutional preparedness. The borderless nature of cyberspace, coupled with weak enforcement mechanisms and low digital literacy, has amplified the social, economic, and moral consequences of cybercrime. This study critically examines the responsibilities of concerned institutions in overcoming cybercrime, with specific reference to Pakistan's legal, administrative, religious, and educational frameworks, while integrating Islamic ethical principles derived from the Quran and Sunnah. The article argues that cybercrime is not merely a technical or legal issue but a multidimensional problem requiring a coordinated institutional response grounded in moral accountability, legal enforcement, and social awareness. It analyzes the roles of government bodies, law enforcement agencies, regulatory authorities, the judiciary, religious institutions, and educational organizations in preventing, detecting, and responding to cyber offenses. Particular attention is given to Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 and (PECA) 2025 highlighting both its strengths and implementation challenges.From an Islamic perspective, the study emphasizes values such as trust (amanah), justice (adl), privacy (ḥurmah al-khuṣuṣiyyah), and accountability (muḥasabah), demonstrating their relevance to contemporary digital conduct. By synthesizing Islamic moral guidance with Pakistan's institutional mechanisms, the article proposes an integrated framework for combating cybercrime effectively. The study concludes that sustainable control of cybercrime in Pakistan requires not only stronger laws but also ethically guided institutions capable of responding to emerging digital threats in a rapidly evolving technological environment.

Key words: *The Holy Quran, the Books of Hadith and The Books of Fiqh.*

Introduction

As the digital sphere increasingly shapes the lives, economies, and communication systems of modern societies, cybercrime has emerged as a formidable challenge that no single institution can address in isolation. The nature of cybercrime is multifaceted ranging from financial fraud and identity theft to online harassment, blasphemy, and cyberterrorism and it often transcends borders, affecting individuals, governments, educational institutions, and private organizations alike. In Muslim-majority countries like Pakistan, where the moral compass is guided by Islamic principles and the constitutional framework affirms the supremacy of Shariah, the response to cybercrime must not only be technically effective but also morally aligned with the values of Islam. Consequently, the fight against cybercrime must be seen as a shared obligation (farḍ kifayah) that enlists the roles of state, Judiciary, Educational institutions, Media, and Religious leadership.

Islamic tradition provides a robust and enduring model of collective moral responsibility (*al-amr bi-l-maruf wa-n-nahy an al-munkar*), which obligates every segment of society to participate in the promotion of good and the prevention of evil. The Quran declares:

﴿وَلْتَكُن مِّنكُمْ أُمَّةٌ يَدْعُونَ إِلَى ا لْخَيْرِ وَيَأْمُرُونَ بِالْمَعْرُوفِ وَيَنْهَوْنَ عَنِ الْمُنكَرِ ﴾[1]

"Let there arise out of you a group of people inviting to all that is good, enjoining what is right and forbidding what is wrong. And it is they who will be successful"

Classical Islamic scholars have interpreted this verse as establishing the collective duty of all institutions religious and secular to uphold ethical order in society. The state, as the central authority, is responsible for establishing just laws and implementing them fairly. The Judiciary must interpret and apply laws with wisdom and impartiality. The Media serves as a powerful tool for shaping public opinion and must be accountable for responsible communication. The Education system is charged with instilling moral, legal, and digital literacy among the youth. Through making good, effective and irrelative curriculum. In this holistic model, institutions become partners in safeguarding society from moral corruption and criminal behavior including that which occurs in cyberspace.

Modern realities, however, have complicated this traditional model. Technological advancement has outpaced legal adaptation, media has become both an informer and a miss informer, and educational institutions often neglect moral instruction in favor of utilitarian training. In Pakistan, while the Prevention of Electronic Crimes Act (PECA) 2016 and (PECA) 2025 both are bound to represent an attempt to regulate cyber offenses, its implementation has been hampered by institutional inefficiencies, lack of coordination, and public mistrust. More importantly, there remains a gap between legal structures and Islamic ethical frameworks, which must be bridged if cybercrime is to be effectively curtailed.

This research thus explores how all sectors of society, guided by Islamic values and legal responsibilities can coordinate efforts against cybercrime. It begins by examining the state, judiciary, media, and education systems as institutional actors (4.2.1), and then analyzes the Prophetic model of collective responsibility in confronting wrongdoing (4.2.2). This is followed by a fiqhi discourse on community safeguards (4.2.3), and concludes with a

[1] *Surah Al Imran :104*

focused discussion on the application of the classical hisbah model in cyberspace (4.2.4). By integrating Islamic jurisprudence, modern case studies, and legal frameworks, this section aims to demonstrate that the combat against cybercrime is not merely a legal or technological endeavor it is a communal moral obligation rooted in the ethical heritage of Islam like Quran, Hadith and enshrined in the responsibilities of all institutions.

Responsibilities of State, Judiciary, Media, and Education Systems:

The prevention of cybercrime in an Islamic society is not a task confined solely to law enforcement or government regulators. Rather, it is a collective institutional obligation grounded in the Islamic principle of societal responsibility (*masuliyyah ijtimaiyyah*) and the modern requirements of inter-agency coordination. The Qur'anic framework for enjoining good and forbidding evil (*al-amr bi-l-maruf wa-n-nahy an al-munkar*) applies not only to individuals but also to institutions that hold public power and responsibility. In Pakistan an Islamic republic where Islam is enshrined in the Constitution this religious imperative extends across four primary domains: the State, the Judiciary, the Media, and the Education system.

1. The Role of State:

The state holds the foremost duty in crafting, implementing, and monitoring cybersecurity policies in accordance with both national needs and Islamic legal principles. The Qur'an commands:

﴿إِنَّ اللَّهَ يَأْمُرُكُمْ أَن تُؤَدُّواْ الْأَمَـٰنَـٰتِ إِلَىٰٓ أَهْلِهَا وَإِذَا حَكَمْتُم بَيْنَ ٱلنَّاسِ أَن تَحْكُمُواْ بِالْعَدْلِ﴾[2]

"Indeed, Allah commands you to render trusts to whom they are due and when you judge between people, to judge with justice"

This verse sets the tone for the state's obligation to ensure both procedural fairness and public accountability. In matters of cybercrime, the state must establish legal structures that protect digital rights, ensure national security, and penalize abuses effectively.

Same as this verse The Holy Prophet PBUH also said:

﴿أَدِّ الْأَمَانَةَ إِلَىٰ مَنِ ائْتَمَنَكَ، وَلَا تَخُنْ مَنْ خَانَكَ﴾[3]

"Deliver the trust to its rightful owner, and do not betray anyone who has betrayed you."

﴿إِنَّ الْمُقْسِطِينَ عِنْدَ اللَّهِ عَلَىٰ مَنَابِرَ مِنْ نُورٍ، الَّذِينَ يَعْدِلُونَ فِي حُكْمِهِمْ وَأَهْلِيهِمْ وَمَا وَلُوا﴾[4]

"Indeed, those who act justly will be on elevated platforms of light before Allah, those who are fair in their judgments, towards their people, and in the responsibilities entrusted to them."

These hadiths emphasize that both **trustworthiness and justice** are fundamental obligations, guiding individuals and institutions to act ethically and fairly in all responsibilities, including governance and cyber-related duties.

In Pakistan, the passage of the Prevention of Electronic Crimes Act (PECA) 2016 represented a landmark step. The act criminalized online harassment, cyberstalking, identity theft, and defamation, and granted enforcement powers to the Federal Investigation Agency (FIA). However, enforcement has faced numerous challenges: lack of technical resources, understaffing, bureaucratic inefficiency, and jurisdictional confusion between provincial and federal authorities. The state must therefore invest in building digital forensics capacity, training specialized

[2] *Surah Al Imran :104*

[3] *Abu Dawud, S. (n.d.) Sunan Abi Dawud, Book of Sales (Kitab al-Buyu'), Hadith 3534*

[4] *Muslim, S. (n.d.) Ṣaḥīḥ Muslim, Book of Leadership (Kitāb al-Imārah), Hadith 1827*

cybercrime units, and establishing dedicated cyber courts. Importantly, all legal reforms should be filtered through Islamic legal principles, ensuring consistency with *maqaṣid al-shariah*.

Islam also emphasizes proactive protection of the public interest (*maṣlaḥah*). Governments should anticipate emerging threats such as cryptocurrency fraud, cyber espionage, and AI-generated disinformation and incorporate them into forward-looking policy. The Prophetic Sunnah illustrates this proactive approach. The Prophet ﷺ established marketplaces where transparency and fairness were maintained by state-appointed officials, who monitored not only commercial fraud but also public discourse. Today's digital marketplaces social media platforms, e-commerce websites, and forums must similarly be supervised under ethical and legal scrutiny inspired by Islamic models.

2. The Judiciary and Its Interpretive Responsibility:

The judiciary plays a crucial role in interpreting laws, adjudicating disputes, and maintaining the moral integrity of the legal system. In Islamic governance, judges (*quḍat*) are not only arbiters of law but also guardians of ethical order. The Holy Quran

﴿وَإِذَا حَكَمْتُم بَيْنَ النَّاسِ أَن تَحْكُمُوا بِالْعَدْلِ إِنَّ اللَّهَ نِعِمَّا يَعِظُكُم بِهِۦٓ إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا ﴾[5]

"And when you judge between people, judge with justice. Indeed, Allah instructs you excellently. Indeed, Allah is ever Hearing and Seeing"

The Prophet ﷺ said:

﴿الْقُضَاةُ ثَلاَثَةٌ وَاحِدٌ فِي الْجَنَّةِ وَاثْنَانِ فِي النَّارِ فَأَمَّا الَّذِي فِي الْجَنَّةِ فَرَجُلٌ عَرَفَ الْحَقَّ فَقَضَى بِهِ﴾[6]

"Judges are of three types: one in Paradise and two in Hell. The one in Paradise is the one who knows the truth and judges according to it"

This Hadith illustrates the immense weight of judicial responsibility.

In Pakistan, cybercrime cases are processed through session's courts or anti-terrorism courts, depending on the nature of the offense. However, the absence of specialized cybercrime benches or Shariah-compliant jurisprudential training among judges has led to inconsistency in rulings. For example, blasphemous content or cyber-defamation cases are often politicized or delayed due to a lack of judicial clarity. Therefore, Shariah training programs for cybercrime judges are essential. Such programs would cover topics like digital evidence in Islamic law, tazir punishments for cyber offenses, and balancing freedom of speech with Islamic norms of modesty and truthfulness.

Furthermore, Islamic law offers a comprehensive doctrine of judicial discretion (istiḥsan) and contextualization (talil), allowing judges to adapt their rulings to changing circumstances. A judge can increase penalties if the crime threatens public order (*niẓam*), or reduce them if there is genuine repentance. This flexibility is essential in digital contexts, where the impact and intent behind actions can vary widely from trolling to terrorism. The courts must also safeguard due process, ensuring that suspects are not punished without valid evidence, false

[5] *Surah Al Nisa:58*

[6] *Al-Tirmidhī, M. (n.d.) Jāmiʿ al-Tirmidhī, Book of Judgments (Kitāb al-Aḥkām), Hadith 1320. [Arabic text*

accusations are not entertained, and victims are provided legal redress. These are not just legal safeguards but also Islamic imperatives.

3. The Media's Moral and Informational Role:

The media both traditional and digital has a profound impact on the cultural, moral, and legal attitudes of society. Its role is twofold: it can either contribute to the spread of cybercrime (e.g., by normalizing immoral behavior or sharing misinformation), or it can become a tool for moral reform, public awareness, and digital ethics education. Islam mandates the careful use of speech and prohibits spreading falsehood, slander, or panic. The Quran warns:

﴿إِذْ تَلَقَّوْنَهُۥ بِأَلْسِنَتِكُمْ وَتَقُولُونَ بِأَفْوَاهِكُم مَّا لَيْسَ لَكُم بِهِۦ عِلْمٌ وَتَحْسَبُونَهُۥ هَيِّنًا وَهُوَ عِندَ ٱللَّهِ عَظِيمٌ﴾[7]

"When you received it with your tongues and said with your mouths that of which you had no knowledge, and thought it was insignificant while it was, in the sight of Allah, tremendous"

In Pakistan, media channels often prioritize sensationalism over substance. Coverage of cybercrime is usually event-based focusing on scandals, leaks, or high-profile cases without providing constructive analysis or ethical education. The media must reclaim its Islamic responsibility by promoting truth **(*ṣidq*)**, privacy (*satr*), dignity (*karāmah*), and justice (*adl*) in its programming. This involves producing content that teaches the public about the legal and religious consequences of hacking, cyberbullying, and misinformation. Talk shows, documentaries, short dramas, and public service messages should include fatwas and references from Quran and Hadith to increase religious awareness.

Additionally, the regulation of online content is a pressing need. The Pakistan Telecommunication Authority (PTA) and Pakistan Electronic Media Regulatory Authority (PEMRA) have attempted to censor inappropriate content but have been criticized for inconsistencies and overreach. A more principled Islamic framework, rooted in *ḥisbah* and *amr bi-l-ma ruf*, can provide ethical guidelines for media regulation without becoming oppressive. This includes blocking pornographic websites, flagging fake news, and banning content that promotes sectarian hate all actions which fulfill both Islamic and public welfare objectives.

4. The Education System's Role in Prevention:

The **education system** is arguably the most critical long-term actor in cybercrime prevention. The Prophet ﷺ said:

﴿طَلَبُ الْعِلْمِ فَرِيضَةٌ عَلَى كُلِّ مُسْلِمٍ﴾[8]

"Seeking knowledge is an obligation upon every Muslim"

This command encompasses not just religious knowledge but also awareness of civic duties, digital responsibilities, and ethical behavior. Today, cybercrime prevention must begin in classrooms both physical and virtual.

Unfortunately, in Pakistan, curricula at most levels lack any substantial modules on digital literacy, cybersecurity, or Islamic digital ethics. Students may use smartphones and social media daily but receive no formal guidance on Islamic etiquette online, the boundaries of legal and illegal behavior, or how to report abuse. There is a dire

[7] *Surah al-Nur :15*

[8] *Ibn Majah, M. (n.d.) Sunan Ibn Majah, Book of Knowledge (Kitāb al-'Ilm), Hadith 224*

need to integrate Islamic cyberethics into school syllabi, especially in religious studies, computer science, and civics. Teaching Quranic verses about honesty, privacy, and respect, along with practical lessons on reporting online threats or protecting one's data, will foster a new generation that is both technically aware and ethically grounded.

Higher education institutions should also introduce courses on cyber law, Islamic jurisprudence, and digital forensics, combining secular legal instruction with Islamic legal theory. Universities like International Islamic University Islamabad (IIUI) and Jamia al-Azhar have the capacity to pioneer such interdisciplinary programs. Additionally, training teachers, imams, and counselors in the basics of cybersecurity and Islamic moral obligations can turn educational institutions into frontlines of digital moral reform.

Researcher comments regarding these institutions:

Each of these institutions the state, the judiciary, the media, and the education system has a distinct but interconnected role to play in preventing cybercrime. Their duties are not confined to policy or enforcement but extend to moral leadership, public education, and the promotion of Islamic values in the digital sphere. The Islamic legal tradition supports such distributed responsibility, emphasizing that justice and moral order can only be upheld when all segments of society work in concert. If Pakistan aspires to build a cyber-safe and islamically principled society, then its institutions must coordinate, legislate, educate, and adjudicate not just with efficiency but with ethical integrity and religious responsibility.

Prophetic Model of Collective Responsibility (الأمر بالمعروف).

The concept of **الأمر بالمعروف والنهي عن المنكر** (enjoining good and forbidding evil) is one of the most foundational principles in Islamic ethics and governance. It represents not only a personal religious duty but also a collective societal obligation that sustains the moral health of the Ummah. The Quran commands,

﴿كُنْتُمْ خَيْرَ اُمَّةٍ اُخْرِجَتْ لِلنَّاسِ تَاْمُرُوْنَ بِالْمَعْرُوْفِ وَ تَنْهَوْنَ عَنِ الْمُنْكَرِ وَ تُؤْمِنُوْنَ بِاللّٰهِ﴾[9]

"You are the best nation produced [as an example] for mankind. You enjoin what is right and forbid what is wrong and believe in Allah"

This divine declaration embeds a universal ethic: that Muslims are divinely tasked with collective moral guardianship over their communities. The relevance of this ethic becomes especially pressing in the age of cyberspace, where evil often proliferates unchecked and the lines between private behavior and public harm are increasingly blurred.

The Prophetic model for fulfilling this duty provides a comprehensive, practical framework that is deeply applicable to cybercrime prevention. The Prophet Muhammad ﷺ said,

﴿مَنْ رَأَى مِنْكُمْ مُنْكَرًا فَلْيُغَيِّرْهُ بِيَدِهِ، فَإِنْ لَمْ يَسْتَطِعْ فَبِلِسَانِهِ، فَإِنْ لَمْ يَسْتَطِعْ فَبِقَلْبِهِ، وَذَلِكَ أَضْعَفُ الْإِيمَانِ﴾[10]

"Whoever among you sees an evil let him change it with his hand. If he is unable, then with his tongue. If he is unable, then with his heart and that is the weakest of faith"

(Sahih Muslim). This hadith delineates a three-tiered strategy for confronting wrong: physical intervention, verbal correction, and internal disapproval all based on the believer's capability. This stratified model provides

[9] *Surah Al Imran :110*

[10] *Muslim, S. (n.d.) Ṣaḥīḥ Muslim, Book of Faith (Kitāb al-Īmān), Hadith 49*

a scalable method for both individuals and institutions to address harm, and it becomes especially useful in analyzing how collective responsibility should function in digital society.

In traditional Islamic society, this principle was not applied haphazardly but through well-regulated roles and authorities. Classical scholars like al-Ghazalı and Ibn Taymiyyah elaborated its conditions: the evil must be clearly recognized by Shariah, the response must not cause a greater harm, and the person acting must be qualified and sincere. Today, as cyber harms such as online slander, pornography, blasphemy, fraud, and misinformation proliferate at unprecedented speeds, the *amr bi-l-ma ruf* principle demands a revival adapted to modern realities. Importantly, this revival must be institutionalized and integrated into all arms of governance, education, technology, and community leadership.

Institutionalizing the Prophetic Model in the Digital Age:

To apply this model effectively to cybercrime, we must first understand how its logic extends to public structures. In classical Islamic governance, the ḥisbah system institutionalized moral oversight. The muḥtasib, or market inspector, was a state-appointed official whose job was to monitor both ethical and commercial behavior in public spaces. He could intervene if people cheated, abused, or harmed others in public view all without requiring a legal complaint. In the online context, this model supports the creation of regulatory bodies that monitor cyberspace for moral violations, such as the spread of fake news, online blackmail, or religious disrespect, even before they result in criminal proceedings.

Modern application of this requires well-trained digital muḥtasibs ethical oversight units equipped with legal, technical, and religious training. Their work must be bound by due process, supervised by independent ethics committees, and sensitive to constitutional rights and Shariah guidelines. For example, if a YouTube channel spreads content that promotes immorality or sectarian hate, such a body could issue warnings, restrict monetization, or even recommend legal prosecution based on Islamic guidelines. This does not contradict freedom of expression; rather, it reaffirms the Qur'anic standard that,

﴿ظَهَرَ ٱلْفَسَادُ فِى ٱلْبَرِّ وَٱلْبَحْرِ بِمَا كَسَبَتْ أَيْدِى ٱلنَّاسِ﴾[11]

"Corruption has appeared on land and sea because of what the hands of people have earned"

Family and Community the First Circle of Responsibility:

Another key dimension of the Prophetic model is its emphasis on proximity and relational responsibility. The Prophet ﷺ said,

﴿أَلاَ كُلُّكُمْ رَاعٍ وَكُلُّكُمْ مَسْئُولٌ عَنْ رَعِيَّتِهِ﴾[12]

"Each of you is a shepherd, and each of you is responsible for his flock"

This metaphorical language assigns every individual a sphere of responsibility, starting with the family and expanding to the broader community. Parents are responsible for what their children consume online, teachers for the moral behavior of students, and scholars for guiding public discourse.

In Pakistan and similar Muslim societies, families are often unaware of the dangers lurking online from inappropriate content to cyber grooming and radicalization. Reviving the Prophetic model requires that families

[11] *Surah al-Rum :41*

[12] *Al-Bukhārī, M. (n.d.) Ṣaḥīḥ al-Bukhārī, Book of Judgments (Kitāb al-Aḥkām), Hadith 893*

receive training and resources to supervise and educate their children. Mosques and community centers can hold workshops on Islamic digital ethics, explaining why cyberbullying violates the Prophet's instruction to be gentle, why sharing unverified content is a form of lying, and why watching immoral content is sinful. This grassroots propagation of enjoining good and forbidding evil can transform communal cyber behavior from the inside out.

Furthermore, community members can be trained to identify signs of digital abuse, offer counseling, or report crimes in a Shariah-compliant manner. Islam commands concealment of private sins but mandates action against public corruption (al-munkar al-ẓahir). The early Muslims considered it a grave failure when evil became normalized without resistance. Applying this to cyberspace means that viral trends promoting indecency, gambling apps and mockery of Islamic figures must be challenged not only by regulators but also by community leaders, educators, and public influencers.

Balancing Collective Duty with Islamic Ethics:

It is vital to stress that the application of *amr bi-l-ma ruf* in cyberspace must adhere to the spirit of justice and compassion. Islam is a religion of balance (*tawāzun*) and wisdom (*ḥikmah*). The Quran says,

﴿ٱدۡعُ إِلَىٰ سَبِيلِ رَبِّكَ بِٱلۡحِكۡمَةِ وَٱلۡمَوۡعِظَةِ ٱلۡحَسَنَةِۖ وَجَٰدِلۡهُم بِٱلَّتِي هِيَ أَحۡسَنُ﴾[13]

"Call to the way of your Lord with wisdom and good instruction, and argue with them in a way that is best"

If applied harshly or unjustly, the collective duty may lead to extremism, privacy violations, or defamation all of which are strictly forbidden in Islam.

For example, exposing someone's private sin online under the guise of enjoining right may actually constitute ghibah (backbiting) or buhtan (slander). Ibn Ḥazm said:

﴿أعظم أنواع الظلم هو ارتكاب الجريمة باسم الأمر بالمعروف والنهي عن المنكر﴾[14]

"The greatest form of oppression is to commit a crime in the name of enjoining good."

This underlines the importance of training those engaged in this duty, especially in the digital domain where messages go viral and reputations are easily destroyed.

Modern jurists emphasize that government institutions, civil society, and educational platforms should facilitate rather than monopolize this duty.

This includes:

- Providing hotlines for reporting digital abuse anonymously.
- Empowering mosques and madaris to teach cyberethics grounded in Quran and Sunnah.
- Encouraging media figures to refrain from content that spreads immorality.
- Training IT professionals in the ethical boundaries of data handling, surveillance, and content moderation based on Shariah standards.

Shariah-Based Precedents for Collective Intervention:

[13] *Surah al-Naḥl :125*

[14] *Al-Ghazālī, A.H. (n.d.) Iḥyāʾ ʿUlūm al-Dīn [The Revival of Religious Sciences], Book on Ethics and Governance.*

Islamic history offers several precedents of institutionalized moral oversight. During the Caliphate of Umar ibn al-Khaṭṭab, it is reported that he sent spies to investigate market fraud and ensure honesty. However, he also emphasized privacy and required clear evidence before prosecution. This balance between intervention and privacy remains critical in addressing cybercrime. While states and communities must not tolerate public corruption, they must also ensure that their methods of intervention are Shariah-compliant.

For example, in handling fake news and online sectarianism, Pakistan's institutions can draw on the example of the Prophet ﷺ, who, upon receiving news of a potential military breach, refrained from acting until verification:

﴿إِن جَآءَكُمْ فَاسِقٌۢ بِنَبَإٍ فَتَبَيَّنُوٓاْ﴾[15]

"If a sinner comes to you with news, verify it…"

This verse forms the Quranic foundation for fact-checking, a practice every journalist, citizen, and social media user should observe. Cyber truth-telling is not just a journalistic ethic it is an Islamic duty.

Fiqhi Discourse on Community Safeguards:

The preservation of social order and moral integrity has always been one of the foundational objectives of Islamic law (*maqaṣid al-shariah*). In the face of cybercrime a phenomenon that transcends traditional notions of space, surveillance, and public accountability there is an urgent need to revive and expand the jurisprudential tools that safeguard the community (*ummah*). Fiqhi discourse on community safeguards addresses how Islamic law empowers both individuals and institutions to act collectively in upholding the public good (*maṣlaḥah ammah*), deterring harm (*mafsadah*), and maintaining ethical discipline in the public domain. This section explores how these traditional principles can be applied to the cyber world, and how communities can be mobilized ethically, legally, and structurally to counter digital harm in light of Islamic jurisprudence.

The Principle of Ḥifẓ al-Mujtama (Preservation of Society):

Classical Islamic jurists such as al-Shaṭibi in *al-Muwafaqat* and al-Ghazali in *al-Mustaṣfā* defined the preservation of society (*ḥifẓ al-mujtamaʿ*) as an extension of the maqaṣid al-shariah. While the traditional list includes preservation of religion (*din*), life (*nafs*), intellect (*aql*), lineage (*nasl*), and property (*mal*), several scholars argue that the preservation of social cohesion and collective morality is embedded within all five. In modern terms, this extends to safeguarding communities against digital harm whether that harm manifests as moral corruption (pornography, hate speech), mental abuse (cyberbullying, blackmail), or communal disunity (sectarian content, online radicalization).

The Islamic legal maxim

﴿ درء المفاسد أولى من جلب المصالح﴾[16]

"Preventing harm takes precedence over securing benefit"

Serves as a foundational guideline in this matter. When applied to community safeguards, it justifies the regulation or even restriction of certain online behaviors, platforms, or expressions if they are proven to damage the collective welfare of the community. For example, online content that promotes inter-sectarian hatred or

[15] *Surah al-Ḥujurat :6*

[16] *Ibn Qudāmah, M. (n.d.) Al-Mughnī, Book on Legal Maxims (Kitāb al-Qawāʿid al-Fiqhiyyah*

blasphemy, even if posted by individuals under the guise of "freedom of expression," may be restricted under Islamic jurisprudence to protect *aqidah* (creed) and community unity.

Taawun ala al-Birr wa-l-Taqwa: Institutional Cooperation in Safeguarding the Ummah:

The Quranic principle of mutual support,

﴿وَتَعَاوَنُواْ عَلَى ٱلۡبِرِّ وَٱلتَّقۡوَىٰۖ وَلَا تَعَاوَنُواْ عَلَى ٱلۡإِثۡمِ وَٱلۡعُدۡوَٰنِ ﴾[17]

"Cooperate in righteousness and piety, and do not cooperate in sin and transgression"

Implies that safeguarding the ummah from digital harm is a communal and inter-institutional obligation. This principle forms the basis for fiqhi models of community partnership, especially between religious institutions, schools, legal bodies, and technology platforms.

In Pakistan, this cooperation remains underdeveloped. Mosques rarely deliver sermons on cybersecurity ethics, schools lack integrated moral curricula, and Islamic NGOs are seldom involved in online moral policing or awareness.

This echoes the *ḥisbah* tradition of classical Islam, where the moral upkeep of society was not left to the state alone but was reinforced by community-level involvement under legitimate ethical parameters.

The Legal Standing of Fard Kifayah in Cybersecurity:

In Islamic jurisprudence, fard kifayah refers to communal obligations that, if undertaken by a sufficient number of people or institutions, absolve the rest of the community from sin. Jurists like al-Nawawi and Ibn Qudamah maintained that if no one fulfills a fard kifāyah, the entire community bears collective guilt. In modern Islamic legal thought, this principle applies powerfully to digital vigilance and reporting of cybercrime.

For example, if a community is aware of an individual who engages in cyberbullying, digital blackmail, or fraud and fails to intervene or report then the sin is collectively borne.

This perspective should inform public policy, particularly in Muslim societies. It also justifies funding state and NGO efforts to promote cyber literacy as part of religious endowment (waqf) initiatives or Zakat-based education projects, as they contribute to the communal safeguarding of religion and honor.

Urf (Custom) and Adat (Cultural Practice) in Cyber Law Enforcement:

Islamic law respects culturally specific practices that do not contradict Shariah, known as *urf* and *adat*. Classical jurists often based judgments on *urf*, provided it served justice and did not violate Quranic boundaries. In cyber law, this allows for regional adaptation of cyberethics, where communal standards are factored into enforcement.

For instance, a village in rural Sindh may find it more socially disruptive to tolerate social media misuse than urban elite in Islamabad. Thus, community-specific norms, as long as they do not oppose the Shariah, may influence judgments on penalties, prevention campaigns, and even what constitutes harm. Local *fiqh councils* should be empowered to evaluate cyber offenses based on Shariah and local context, particularly in cases involving minors, family honor, or interfaith relations.

Fatwa Mechanisms and Cyber Crisis Response:

[17] *Surah al-Maidah :2*

The fatwa system in Islam has always played a key role in offering guidance to the community on emerging issues. In light of new technologies, several Islamic councils including the International Islamic Fiqh Academy and Pakistan's Council of Islamic Ideology have issued rulings on digital topics ranging from online privacy, crypto currency, pornographic content, and cyber fraud.

Application of Hisbah in Cyberspace:

The classical Islamic institution of ḥisbah was established to safeguard public morality, uphold justice, and prevent societal harm by empowering an appointed authority to intervene in matters of public wrongdoing. Rooted in the Quranic command

﴿وَلْتَكُن مِّنكُمْ أُمَّةٌ يَدْعُونَ إِلَى ٱلْخَيْرِ وَيَأْمُرُونَ بِٱلْمَعْرُوفِ وَيَنْهَوْنَ عَنِ ٱلْمُنكَرِ ﴾[18]

"Let there arise among you a group who invite to all that is good, enjoin what is right and forbid what is wrong"

The ḥisbah system served as a mechanism for regulating markets, behavior, and community order. In our digital era, where cyberspace represents a vast public sphere with minimal regulation, the revival and modernization of ḥisbah principles offer a powerful and Shariah-compliant framework to combat cybercrime, reinforce digital ethics, and promote community well-being.

Qualifications and Ethical Parameters of Cyber Muḥtasibs:

A vital component of hisbah is the **moral integrity and scholarly competence** of the muḥtasib. Al-Mawardi emphasized that the muḥtasib must have knowledge of what is legally required and forbidden, be just in character, and avoid partisan or tribal bias. In cyberspace, the ethical risk is even greater: digital surveillance, public exposure, and online denunciation can lead to slander, unjust accusations, or reputational destruction.

Therefore, the cyber muḥtasib must be:

- Trained in Islamic law, particularly *ḥisbah*, *ḥudud*, *ta zir*, and *usul al-fiqh.*
- Technologically literate, capable of understanding coding, content filters, data flow, and app functionality.
- Accountable to a Shariah-compliant oversight board.
- Bound by a strict privacy protocol, ensuring that evidence is not shared irresponsibly.
- Prohibited from acting on rumors, anonymous accusations, or political instructions.

Hisbah in cyberspace must not become a tool for religious authoritarianism or political surveillance. It must be rooted in public interest, ethical moderation, and compassion reflecting the Prophet ﷺ's balanced enforcement of justice and mercy.

Comparative Case Studies of Modern Hisbah in Practice:

Countries such as Saudi Arabia and Nigeria have experimented with modernized forms of hisbah. In Saudi Arabia, the *Committee for the Promotion of Virtue and Prevention of vice* (CPVPV) historically performed offline monitoring duties, although reforms have limited its direct enforcement. In Nigeria's Kano State, the Hisbah Board actively patrols markets and media, ensuring compliance with Islamic moral standards. These models, while not without criticism, offer practical insights into institutional design.

For Pakistan, rather than physical policing, the emphasis should be on:

[18] *Surah Al Imran :104*

- Digital ethics education.
- Content flagging systems.
- Public shaming avoidance.
- Victim protection.
- Legal safeguards against abuse.

Such an approach would combine Islamic authenticity, social acceptance, and procedural justice.

Conclusion:

The revival of the ḥisbah system for cyberspace is both timely and necessary. It provides a uniquely Islamic response to the challenges of moral degradation, digital crime, and online disorder. By adapting the ethical, legal, and structural components of classical hisbah to the realities of cyberspace, Muslim societies can reclaim agency over their moral future.

Hisbah is not about policing piety it is about creating a culture of ethical vigilance grounded in compassion, truth, and justice. In cyberspace, where anonymity breeds abuse and silence permits oppression, the principle of enjoining good and forbidding evil must be institutionalized, digitized, and humanized. Pakistan, with its constitutional mandate and Islamic legal tradition, is well-positioned to lead this revival crafting a model where cyberspace becomes not just lawful, but morally enlightened.