Exploring cybercrime history through a typology of computer mediated offences: Applying Islamic principles to promote good and prevent harm

Syed Raza Shah Gilani[1], Bahaudin Ghulam Mujtaba[2,*], Shehla Zahoor[3], Ali Mohammed AlMatrooshi[4]

[1] *Abdul Wali Khan University Mardan, Mardan 23200, Pakistan*

[2] *Huizenga College of Business and Entrepreneurship, Nova Southeastern University, Fort Lauderdale, Florida 33314-7796, USA*

[3] *Assistant Professor of Law, Shaheed Benazir Bhutto Women University, Peshawar 25000, Pakistan*

[4] *Dubai Police-General Department of Human Rights, Brunel University of London, UB8 3PN Uxbridge, UK*

*** Corresponding author:** Bahaudin Ghulam Mujtaba, mujtaba@nova.edu

ARTICLE INFO

Received: 11 November 2023
Accepted: 30 November 2023
Available online: 26 December 2023

doi: 10.59400/cai.v1i1.321

ABSTRACT: By the new century, the sheer complexity and number of reported cybercrime incidents had exposed major flaws in the cybersecurity infrastructure of industry giants, as well as governments. For example, there have been numerous attempts to intercept Google's source code for the purposes of extracting confidential commercial data. National authorities were also slow to respond to the distribution of offensive images or copyrighted materials over the internet. While previous threats were mostly localized to certain computer systems, in particular countries, the emergence of the modern financial system has transformed digital crimes into a transnational phenomenon. In the intervening years, several companies, such as Lloyds in 2015, have been targets of financial hacking operations. The loss associated with cybercrime has been escalating annually, with figures indicating that costs borne by companies had quadrupled between the years of 2013 and 2015. The challenge has become worse in the recent years and artificial intelligence applications can create even more complexity and anxiety for professionals in every workplace. So, this trend of cybercrimes growing rapidly in the era of artificial intelligence is likely to affect developing and transnational economies, as more public and private sector banking institutions conduct their services online. Muslim countries must jointly collaborate, discuss, and link their spiritual principles to guard against, discourage, and prevent cybercrimes. Implications for Islamic nations along with their public and private sector leaders are explored in this manuscript.

KEYWORDS: cybercrime; criminal intend; online fraud; transnational cybercrimes; Islamic principles; data espionage; crackers; hackers

1. Introduction

Every day, we see new innovative technologies being introduced and used to fulfill professional goals and personal dreams. Some people use new technologies for efficiency and productivity, while others use them for cybercrimes or to cheat and/or shortcut their assignments[1], since modern artificial intelligence (AI) tools "can generate full documents, summarize historical events, create art—in simple terms, and 'complete your homework for you'". AI tools can mimic human cognitive capabilities and functions often more quickly than teams of professionals, which means cybercrimes can often go undetected for hours and days. Therefore, modern professionals must be aware of cybercrimes and take proactive measures to prevent it through a multi-pronged approach which can include spiritual values. As such, this article examines the history and definition of cybercrime in contemporary debates as the backdrop against which the study will analyze how such crimes are being combated and prosecuted in various countries, especially in Islamic nations such as Pakistan, Iran, Indonesia, Malaysia, Jordan, Egypt, Nigeria, and others. While the article concludes by returning focus to legal and cultural perspectives on cybercrime, the focus is on key issues, definitions, and challenges associated with emerging cybercrime and identity theft phenomena which are impacting people all over the globe[2]. To this end, and in line with the aim of addressing the effectiveness of a developing nation's cybercrime legislation in tackling the growing trend in identity theft related offences, the paper begins with a brief overview of the legal and policy implications of the world's increased dependency on information technology. We will explore several Islamic principles that can be applied by public and private sector leaders to promote "good" through the cyber environment and prevent harmful activities in the modern tech-savvy world, where "the internet of things" are critically influential.

Of course, artificial intelligence technologies are allowing more tools and opportunities for scammers to take advantage of people in all societies regardless of religion or economic prosperity. Westfall[3] explains that "AI voice-cloning scams are on the rise", and these scams are very disturbing because they work and can confuse people who are tech-savvy. As such, individuals as well as public and private sector leaders must protect themselves and their constituencies. In the United States of America.

The Federal Trade Commission warns that scammers are using artificial intelligence to clone people's voices, and the crimes are leading to distressing situations for people around the country. Criminals are tricking victims into thinking they're talking to a relative who may need money for reasons like paying for damages from a car accident, or paying ransom for a kidnapping. Criminals just need a 20-second clip of someone talking, which is often pulled from social media, and they can make an eerily similar clone of their voice. All the way to the point that a mother can't tell the difference between her own child, and a machine[3].

2. Historical view of cybercrime

The global cybercrime market is a low-risk, high-return criminal enterprise, with goods and services in strong supply and demand. As a matter of fact, anyone aiming to make an illicit profit can purchase infrastructure, delivery mechanisms, coding services, antivirus checking services, exploit kits, communication services, and 'cash out' and money transfer services. The challenge lies in detecting the constantly evolving illicit activity, and determining its motivation, impact, and mitigation strategies in real time since criminals learn and adjust their techniques continuously[4].

The term "cybercrime" was not widely used until the late 1990s. However, the practice and method of interfering with information technologies have been in existence for more than a century. The first hacking incident was recorded in 1878 and involved the interception of phone lines through a device known as phreaking. The first recorded example of computer hacking occurred in the 1950s with the use of large mainframe computer servers. At that time, only 13 computer offences were reported worldwide. Criminal prosecution of these crimes was for the most part focused on offences involving the physical theft and destruction of computer hardware rather than "virtual" crimes affecting computer software and information networks[5].

By the mid 1960's, authorities in the U.S. had begun trials on a new electronic database that would allow for information to pass between governmental agencies. The relevant American authorities recognised that although the creation of a centralised governmental database would allow agencies to obtain and record information more efficiently, it would also generate significant privacy and accessibility concerns[6]. As a result, a newly created data authority proposed that new legislative provisions address the potential misuse of private information. These early policy debates in the 1970s rose to greater prominence in subsequent decades as companies and governments begun to rely on information databases[7].

By the 1980s, the speed and operability of computer processors had vastly improved. Now faster and cheaper, computers were widely used in the private sector. Financial markets were also reliant on predictive software and applications that aimed to eliminate human error. Banks were now a repository of financial data belonging to thousands of customers. It is a small wonder that this period sparked a rise in online fraud, software piracy, and network related crimes. Information networks would emerge as an ideal environment for crime because of the anonymity they provide to would be criminals[4].

This period also brought a paradigm shift in legal discourses, marking a move away from traditional property related conceptions to new conceptions and categories of virtual "crime", including illegal use, manipulation and interference with electronic data and information systems. The terminology of "hacking" was popularised during these periods, as offenders exploited flaws in firewalls to gain unauthorised access to computer networks without having to be physically present at a "crime scene". A single use of malicious software could be used to infect and disrupt globally integrated information and payment systems. Faced with the financial costs and dispersive effects of network-disabling cybercrimes, national legislators were forced to reconsider existing definitions and enforcement strategies. In the United States, once a leader in the push-back against cybercrime, the Comprehensive Crime Control Act (CCCA) was drawn up and passed. Subject to this Act, national security agencies were given new jurisdictional powers over cases of computer and credit card fraud. In 1986, two other cybercrime-related laws were passed in the United States—the Computer Fraud and Abuse Act (CFAA) and the Communications Privacy Act (CPA), each outlawing unauthorised access to computer systems as a criminal act[8].

Despite legislative developments in the United States and the United Kingdom, cybercrime continued to make headlines. In 1988, a self-replicating computer virus known as the I-Love-You Virus, infected over 6000 computers worldwide. These actions prompted crime agencies such as INTERPOL to propose several measures aimed at fostering joint responses on threat and crime detection and enforcement[9]. One of these recommendations called on national governments to establish a local Computer Emergency Response Team (CERTs)—a body assigned with the task of anticipating and notifying global counterparts of large-scale attacks on computer networks. The U.S. and the U.K., as well as many other countries, set up national CERTs in response to these recommendations.

The 1990s culminated in an explosion of the global information highway. The territorial boundaries that had long separated nation states no longer applied in cyberspace now that the publication or use of information in one country could be treated as a criminal offence in another. Hacking incidents also increased in frequency and significance during this period. In 1994, hackers accessed major government servers such as NASA and the Korean Atomic Research Institute. In the same year, an employee of a British Telecom illegally trespassed into a network containing information relating to secret military installations. The year 1995 marked another turning point in joint-level law-enforcement responses to the rise in online financial hacking incidents, culminating with the arrest of Vladimir Levin who was alleged to have stolen an estimated $3 to $10 million from Citibank. The disruptive power of “hacktivist” organisations such as Wikileaks and the leak of thousands of diplomatic cables would, in years to come, sharpen public awareness of data breaches involving sensitive information[10].

Today, most experts agree that cybercrime can include numerous activities, including phishing, spear phishing, and whaling or using fake email messages to get another individual’s personal information from internet users or from corporate data networks[11] by targeting specific individuals. It can also include hacking into corporate databases and even shutting them down or misusing their websites, computers, and employee or customer credit card numbers. As such, all individuals, corporations, and governments must work to prevent these hackers from accessing their sensitive data since cybercrimes are on the rise[12]. In a press release by the U.S. Attorney’s Office of Western District of New York, it is mentioned a 24-year-old by the name of Maurice Sheftall from Brooklyn, NY, pleaded guilty to fraud and related activities in connection with hacking of corporate computers and stealing customer data. He was sentenced to three years of probation and paying restitution totalling to $41,441. Apparently, Sheftall illegally obtained the customer credentials, such as logins and passwords, for more than 50 customers that had opened accounts with the supermarket retailer known as Wegman. Sheftall logged into Wegman’s customers’ accounts and changed their passwords and e-mails, thereby locking customers out of their accounts. He used their credit card information to buy groceries for himself and his employees. During a five-month period in early 2021, Sheftall defrauded Wegmans and many of their customers by placing fraudulent orders, in the amount of approximately $9297. The supermarket’s actual losses amounted to $41,441 as they reimbursed their customers, purchased credit monitoring for customers who were victims of this hacker, and “the purchase of dark web monitoring to determine where and how Sheftall obtained the customer account information he used to access the accounts”[13]. The Federal Bureau of Investigation (FBI) investigated this cybercrime which eventually led to the guilty plea by Maurice Sheftall.

The historical review of literature shows that the misuse of information technology is by no means a new or novel problem. Governments have been forced to develop laws and legal measures to address the abuse of technologies since even before the internet was invented. However, these responses have not always been effective at addressing new challenges, due to the evolving ways in which computer and network related offences are committed. This is because the internet makes it possible for a person to attack the integrity, confidentiality and privacy of computers and computer data from virtually any place in the world. The identity of the offender is often difficult to establish, and even when law enforcement agencies have enough evidence to indict a person, they may be unable to establish *personal or in rem* jurisdiction (which is the authority of a court over property) to bring criminal proceedings against the offender.

There is consequently a pressing need for legal concepts and frameworks that can both prevent online risks as well as deter future offenders by the threat of criminal prosecution and punishment. The first relies on effective cooperation between law enforcement, at the domestic and international levels, and industry leaders in the field of cybersecurity. The latter depends on the existence and adaption of outmoded criminal law definitions to reflect enforcement challenges. The next section will delve more deeply into these issues as viewed through the prism of identity theft offences[14].

2.1. Definition of cybercrime

There is no singular or universal definition of cybercrime, and the term has attracted broad and narrower definitions. Cybercrime describes any illicit activity performed using electronic operations that violate the confidentiality, integrity, and availability of computer systems, including the data stored on digital devices[15]. As digital methods become ever-more sophisticated, the definition and ambit of legal regulations have been expanded to include offences that are made possible only with the use of computers, or what we might call computer-centric crimes. The broadest definitions of cybercrimes are drawn expansively to include crimes against the person, property, and national governments. Crimes against internet activities do attract global condemnation and punishment, such as the distribution of child pornography and cyberstalking[16] and crimes against government cyber warfare and terrorism[17]. The more well-established category of crimes is against property including intellectual property violations and software piracy, as well as online account takeover. The traditional delineation of crimes breaks down when it comes to certain computer-mediated offences. An offence such as financial identity theft could foreseeably be classified as a crime against a person and as a crime against property, depending on how one defines the property, or assesses the "true" victim of online financial fraud (is it the bank, or the customer?). Moreover, data breaches, including hacking and data interception, described below, cannot be easily accommodated by traditional theories on property theft. These breaches clearly infringe on the privacy of the data owner. To classify such acts as "theft" of the property would, however, involve "stretching" the common meaning and usage of these terms to their legal and linguistic limits[18].

In the age of information, there is a need to continuously assess whether national legislation is suitably adapted to take account of these a-typical crimes, where traditional definitions no longer work. The next section will consider these issues in the context of attempts to develop a new taxonomy of data related offences.

2.2. Criminal intent in cybercrime

As alluded to above, the emergence of new and increasingly obscure forms of computer-based crimes has challenged our traditional understandings of criminal activity and intent. Under the usual tests of criminal law, a crime can only be sanctioned by law when the a) subjective element of criminal intent (*mens rea*) can be demonstrated beyond a reasonable doubt, in conjunction with b) the objective test of having committed, or been complicit in, an act or conduct (*actus reus*) proscribed as a criminal offence under the relevant laws of a given legal system. What then counts as criminal intent in the context of "computer crime"?[19].

The evolving categories of the computer-mediated crime described above may be difficult to reconcile with traditional conceptions of a crime done to a "thing" or person. While there is sufficient case law on both sides of the Atlantic to support the notion that the theft of intangible information is prohibited in the same way theft of physical property is, jurisdictions such as Saudi Arabia apply different legal principles to these issues. Under Saudi Arabia's Islamic law governed system, certain conditions must be fulfilled before an offence can be classified as theft. One of these is that the property stolen must be capable of physical ownership. It is quite plausible to argue that this is a proper application of the law given that criminal law and penalties should be reserved for serious offences which produce substantial harm, loss, or injury to an individual or the public[20].

The conceptual challenge of redefining criminal law to "fit" new types of computer crimes is not a problem that is unique to Islamic legal systems. In the age of big data, where more and more of our private information is stored online, there is a burgeoning debate around the illegality of data breaches, raising questions around the dividing line between the mishandling of personal information and deliberate acts of destruction, trespass, theft, and deception for financial gain. In this regard, the motivation of cybercrime offenders varies greatly. Some offenders seek to gain notoriety by circumventing the cybersecurity systems of governmental agencies or tech giants such as Google. Other organisations such as Wikileaks profess more noble aspirations that include improved transparency, democracy, and accountability of governments to the general public. How far should these issues of establishing intent and liability, therefore, be left to the discretion of national legislators and courts? On the broader issue of adapting to criminal law definitions to the new digital landscape, it has been noted that.

Generally, legislators will only prohibit human acts if that is consistent with existing laws and the penal philosophy responsible for them. Most of the computer crimes are consistent with existing legal prohibitions and the penal philosophy responsible for them. Illegal access is the electronic version of trespass. Illegal interception can be seen as an electronic invasion of privacy or burglary offence. And data interference is an electronic property damage offence. System interference and the misuse of devices are entirely new offences that have no analogue in traditional crime, however, system interference protects an entirely new legal interest that has been brought about by the advent of computer systems: the interest of operators and users of computer systems to be able to have them function properly[21].

The above quote raises a fundamental question: whose interests should cybercrime legislation serve: business operators, governments, or individuals? After all, the legal interest of an individual whose credit card details may have been "stolen" can conflict with the credit card company that has suffered a system breach. Normatively speaking, one could also criticise the claim that the legal interest being served by emerging computer crime legislation is to "have them function properly". This seems to be an overly narrow conceptualisation of the law's potential role in regulating the uses and misuses of technology. Moreover, why should certain offences be treated as analogues of traditional crimes, while others are framed in more functional, neutral, and technical terms, as though system or data offences do not also implicate highly contentious matters of national law and policy?

There are conflicts between how the law should balance among competing interests, for instance, the website operator's ability to maintain access to commercial and communications networks and the customer's legal rights to own and control data identifying them. How regulators draw these legal distinctions reflect policy, rather "neutral, choices on matters of criminality, privacy, and security". It is also not entirely clear that these offences can be treated as discrete offences, and indeed there is a significant overlap between computer-mediated offences. At the same time, the divide between traditional and anomalous methods of online crime can be overstated, since modern forms of cybercrime involve elements of both[22].

3. Computer centric crimes

There have been several attempts to formulate a definition of cybercrime that goes beyond the usual penal categories of national criminal law. To this end, Article 1.1 of the Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (the "Stanford Draft") offers a broad definition as any action that involves an illicit use or trespass on a "cyber system". The Council of Europe Convention on Cybercrime goes further to develop a typology of computer and network related offences. Under this framework, four main categories of crimes are identified and differentiated as punishable offences. These are offences against the integrity and accessibility of computer systems and data, computer related offences, copyright related offences, and content related offences. As noted in a report by the International Telecommunications Union, these categories overlap in several ways since they are not "based on a sole criterion to differentiate between categories". The next section will briefly describe the main variants of computer-mediated offences with a view of examining the relationship between data offences and the broader definition of identity theft[23].

3.1. Illegal access

The unauthorised or illegal access to a computer is the oldest and perhaps most immediately recognisable form of cybercrime. This category would include hacking and related offences involving unlawful access to a computer system[24]. As indicated above, hacking is one of the most common and destructive types of cybercrimes. Legally, hacking is defined as a mode of trespass or intrusion on computer systems and network resources through the exploitation of network security vulnerabilities. Hacking may be carried for the purposes of acquiring personal information to commit a crime, to deface websites, to conduct an attack to an entity, and for other criminal purposes including financial fraud.

From the perspective of criminal law, it is necessary to bear in mind that hacking offences are rarely an isolated event. Hacking offences are usually accompanied by preparatory acts such as the use of malware. The use of corrupt hardware or software is intentionally implemented or transferred to the targeted computer so that the hacker can gain access to, or override, security related applications such as password prompts. Cracking has been identified as a new variant of hacking related offences. In essence, cracking describes a technique whereby offenders use their skills to reverse engineer software programs, thereby exposes the computer system to malicious elements such as viruses, which may be inserted into the computer's signature code. System crackers are those who have special expertise in targeting operating systems to exploit network vulnerabilities. For example, system crackers carry out interactive searches to find defects in the security of operating systems and network protocols.

An analysis of different jurisdictions highlights divergences in regulatory approaches. Some jurisdictions confine criminal law sanctions for illegal access related offence to the most severe cases. Relatively minor cases of hacking lacking the intent to bypass security protections, cause harm, or destroy data do not meet the threshold of criminal liability under the applicable national law. Other legal systems adopt a strict liability approach and criminalise any form of unauthorised access[25].

3.2. Illegal data acquisition and data espionage

Closely related to the offence of illegal access is the overlapping "crime" of illegal data acquisition. Data espionage refers to any deliberate act of acquiring personal or sensitive data without the owner's consent. Trade secrets and other commercial data are a frequent target of data espionage offences. Corporate espionage is also recognised as a sub-category cybercrime, whereby rival companies and criminal networks illegally access and trespass on closed private networks to acquire trade secrets or exploit copyrighted works.

Data espionage can be accomplished through viruses and spyware, collectively known as malware. There are numerous types of spyware available on the market, for instance, keylogging applications. Once installed on a computer, key logger applications can record important security information such as passwords. Keylogging software can also be attached to computer hardware, namely the keyboard, enabling sensitive data to be recorded and transmitted to third parties.

Overall, hardware-based spyware is more difficult to install since the offender must physically attach it to the victim's computer. On the other hand, remote forms of spyware are exceedingly hard to detect. This points to the general obstacles faced by local law enforcers engaged in efforts to locate and successfully prosecute anonymous offenders. In contrast with earlier prototypes, viruses can be circulated to a wider reach of victims through the internet, most commonly through "infected" email attachments or “downloadable” files. These viruses are rapidly disseminated because offenders can gain remote access to, and subsequently, control, destroy and delete program files[22].

3.3. Data interference

Data interference offences are singled out as another variant of computer-mediated crimes. By modifying or altering computer files, interfaces and system programs, offenders can inflict significant damage to business operations simply by disrupting company access to data in their possession. Businesses will increasingly rely on information systems to rapidly access, retrieve and collect data to effectively administer and manage accounts and track market trends. The volume and availability of data on computer systems, however, risks the integrity of that information. This is because offenders have a greater opportunity to intercept and monitor private communications between users, such as email communications. They can do this by gaining unauthorised access to wireless or fixed-line communication ports, or by finding unsecure routes through chat functions or other virtual communications. Offenders call also intercept non-encrypted information from data transfers stored on cloud computers or other external storage media available on the internet. The offender may use these functions to blackmail individuals or businesses by locking them out of files until a “ransom fee” is paid.

For the above reasons, many legal systems have amended their penal codes to include data acquisition offences. In addition, there have been attempts to enact robust data protection and privacy laws which regulate the conditions under which internet service providers (ISP) or other media platforms store and transfer information relating to individuals. The European Union, for instance, requires companies to obtain the consent of the data subject (the person who the data relates to) before collecting, using, or transferring that information to third parties[26].

3.4. System interference

Scholars have also drawn a nuanced distinction between data and system interference offences. The former describes efforts to delete, alter or deny access to personal files and data. The latter describes attacks against computer systems, including physical attacks on computer hardware. Damage of this kind would fall under traditional definitions of destruction and damage to property. In recent years, system interference offences typically refer to computer systems which are launched remotely, for instance, computer worms and denial of service attacks. Worms inflict damage on computer networks by creating self-replicating programs that disrupt communication channels, for instance, overloading the network with traffic, causing websites to crash. Computer worms can, consequently, result in significant losses to the business that are unable to operate or trade as normal. While worms can be targeted at entire computer networks, “denial of service” attacks are targeted at a specific computer rendering them inaccessible to the intended victim for several hours and days. System interference is most often accomplished through the spread and proliferation of malicious viruses or spyware in the organization’s operation[27]. Companies and individual users that have neglected to install up-to-data anti-malware detection and prevention software are soft targets for this type of offence[28].

The key conceptual challenge presented by system and data related computer-mediated offences lies in their ‘virtual’ and instantaneous nature. With the rise of automated software attacks, offenders no longer need to have physical access to a computer to able to acquire private data. By the time illegal access has been obtained and data extracted without consent, the offender may already have engaged in further offences of fraud or theft. Since these offences occur remotely and often in jurisdictions that do not benefit from robust cybercrime laws and enforcement regimes, the likelihood that offenders will be successfully apprehended and brought to justice is, at times, exceedingly low. Nonetheless, many employers have instituted policies that specify that employees should not expect privacy in public spaces as all company properties and equipment are being monitored[29].

4. Virtual offences and law

Should virtual offences be brought under the scope of criminal law? The Council of Europe Convention on Cybercrime has attracted the most signatories and consequently can be seen to represent a broad-based political consensus among states around emerging norms and principles of cyber law. Despite its emerging status as customary law, the Convention does not definitively settle debates on what should or should not count as a crime. Instead, cybercrime is defined in circular terms as any unlawful computer related activities which are conducted through global electronic networks. Of course, this only begs the question of what types of activities should be prohibited and are, moreover, sufficiently harmful to justify criminal proceedings and penalties. Moreover, by focusing exclusively on acts committed through "electronic networks", the Convention appears to exclude certain forms of physical theft or destruction. This is problematic because online fraud can occur after a theft of a physical item such as a credit card or documentation containing personal information. Moreover, this definition excludes the use of physical devices used to "export" software that destroys data stored on a computer. This is problematic because the act of storing this virus and transferring it to another person's physical property clearly implies malicious intent on the part of the offender[30].

Other legal instruments provide for a technical definition of cybercrime as covering any situation where a computer or information network is used as the tool, or target, of criminal activity. The cybersecurity company Symantec defines a cybercrime as any act of crime committed using a computer, network device or hardware. This definition is clearly formulated with the crimes of data acquisition, illegal access, and data interference in mind. Many of these offences overlap: a hacking offence often precedes or facilitates some further act of data interference or espionage. For example, the use of malware installed through hacking techniques may also be used to aid and abet a more serious act of theft or fraud.

In the broader scheme, there are inherent difficulties with any definition that brings within its scope any activity involving the use of computer or technological tool, no matter how tangentially. The most absurd application of an over-inclusive definition of cybercrime "would, for example, cover traditional crimes such as murder, if perchance the offender used a keyboard to hit and kill the victim". A more sensible criticism, rather than an overly broad definition of cybercrime, is that it sheds no further light on what kinds of uses of a computer are sufficiently serious in purpose and intent to give rise to criminal liability and emotional distress[31]. Put differently, technical, or industry lead definitions place undue emphasis on the methods used to commit "computer-related offences" rather than the object of legal protection or the harm intended. A further difficulty with an imprecise definition of cybercrime is that national authorities are left with a wide margin of discretion to determine what counts as illegal or illicit activities[32–34]. The next section explores how Muslims can mitigate the risk of cybercrimes through their spiritual values.

5. Islamic principles and cyber crime

In the context of contemporary problems like cybercrime in the modern workplace, Islamic teachings do provide instruction on ethical conduct and morality as a source of inspiration. Even though traditional Islamic law (*fiqh*) may not address cybercrime directly, certain basic concepts may be utilized to handle a variety of problems related to cybercrime. The following are some Islamic precepts that may at different times apply to online criminal activity.

Private (*Sitr*): Islam puts a significant emphasis on respecting one's own as well as others' honor and dignity, as well as maintaining one's own privacy. These principles can be violated in several ways, including unauthorized access to personal information, hacking, and cyberstalking. The act of stealing or fraudulently accessing another person's digital assets, financial information, or personal data is forbidden in Islam. This is known as the "*prohibition of theft*", or "*sariqah*". This is in addition to the fact that actual theft is also forbidden in Islam. The act of spreading false information through social media, participating in online defamation, or establishing phony accounts with the intention of misleading others goes against the Islamic values of honesty and truthfulness, and thus it is forbidden (*Tafsir*).

Prohibition of backbiting (*Ghiba*): Contrary to the Islamic prohibition of backbiting and injuring others, engaging in cyberbullying, online harassment, or utilizing technology to insult, slander, or damage people is considered a violation of this ban. Honoring agreements and honoring the terms of service of online platforms and services is consistent with the Islamic ideals of honesty and trustworthiness. This concept is referred to as *amanah*.

Principle of non-injury (*Istislah*): Islam places a strong emphasis on non-injury (the principle of non-injury), both to oneself and to others. This concept is violated when one commits acts of cybercrimes that are harmful to people, organizations, or society.

Promote good and prevent harm (Amr Bil Maruf wa Nahi Anil Munkar): Islam urges people to encourage good activities and discourage bad ones. This concept is known as "promotion of good and prevention of evil". In accordance with this idea, the reporting of cybercrimes and the prevention of harmful online activity is required of all Muslims. Engaging in cyberbullying, sharing personal information without authorization, or propagating nasty stories online may be regarded as a type of gossip, which is forbidden in Islam. Another form of speech that is forbidden in Islam is known as *gheebah*.

Respect for authority and the law (*Ta'a*): Adhering to the laws of the nation, particularly those pertaining to cybercrime, is consistent with Islamic teachings about the need to maintain justice and honor authority. Plagiarism, the unlawful dissemination of copyrighted information, and software piracy are all acts that go against the idea of protecting intellectual property rights, which is referred to as *istihqaq*. It is essential to keep in mind that different Islamic scholars and communities may arrive at different interpretations and implementations of Islamic teachings. It is possible that Muslim countries and experts need to collaborate to update these principles for the modern times and provide recommendations that are particular to cybercrimes. Additionally, measures to prevent and treat cybercrimes should be carried out within the context of existing legal systems and international agreements, taking into consideration the unique characteristics of the digital world.

In closing, it should be noted that addressing modern-day cybercrimes within Muslim nations or diaspora requires a holistic approach that incorporates Islamic principles, legal frameworks, technological advancements, education, and international cooperation. By embracing a comprehensive strategy, Muslim nations can effectively combat cybercrimes while upholding the values and ethics of Islam. Respecting individual privacy, preventing harm, promoting honesty, and upholding justice are key principles that Islam emphasizes and that can guide efforts to combat cybercrimes. Developing and updating legal frameworks to encompass a wide range of cyber offenses while considering Islamic values will help create a strong foundation for law enforcement to tackle these issues effectively.

Public awareness campaigns and educational initiatives that align with Islamic teachings can empower individuals to use digital platforms responsibly and ethically, thereby contributing to a safer online environment. Collaboration with technology companies and international organizations will enable sharing of expertise, resources, and information to combat transnational cyber threats. Ultimately, the challenge of modern cybercrimes calls for a balanced approach that combines the ethical teachings of Islam, the dynamism of technology, and the cooperation of diverse stakeholders. By embracing these principles and working together, Muslim nations, through public and private sector leaders, can pave the way for a digital landscape that aligns with Islamic values while ensuring the security and well-being of their citizens in the digital age.

6. Summary

In terms of overall value and contributions, this article has offered an exploration of the current definitions and debates on cybercrime, focusing on identity theft offences. In the age of the internet, the integrity, confidentiality, and security of personal data is increasingly at risk. Internet users often exercise little control over how that data is used. These difficulties exist regardless of whether the site of regulation is national, international, or business level. Identity theft offenders have shrewdly deployed social engineering techniques such as phishing to steal personal information. The personal information obtained is then used to further deceive their victims. Perhaps more than other types of cybercrime, identity theft can only be effectively regulated if data protection and security are jointly addressed.

Developing countries often lack the regulatory capacities to effectively address new cyber threats or track down and prosecute criminal operations and networks. Islamic countries may need to revise their cybercrime laws to address these deficiencies, particularly in the areas of data protection and privacy. A priority must be to increase the strength of deterrence through effective policing and enforcement strategies for addressing identity theft. However, the types of identity thefts that have generated most attention in the financial arena are those that have targeted prominent governmental representatives and culturally significant institutions. Moreover, all regulation, in Muslim nations, needs to be evaluated on the backdrop of the Islamic law that governs aspects of criminal law.

Ethical approval

All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Informed consent

Informed consent was not applicable in the study.

Author contributions

Conceptualization, SRSG; methodology, SRSG; software, SRSG; validation, SRSG, BGM, SZ and AMA; formal analysis, SRSG, BGM, SZ and AMA; investigation, SRSG; resources, SRSG; data curation, SRSG; writing—original draft preparation, SRSG; writing—review and editing, SRSG, BGM, SZ and AMA; visualization, SRSG, BGM, SZ and AMA; supervision, SRSG; project administration, SRSG, BGM, SZ and AMA; funding acquisition, SRSG. All authors have read and agreed to the published version of the manuscript.

Funding

There was no external funding for this research. It was self-funded by the authors.

Conflict of interest

The study authors declare that they have no conflicts of interest.

References

1. Hoeck T. Artificial intelligence is here. Available online: https://lecnews.nova.edu/mass-mail/artificial-intelligence-is-here/ (accessed on 21 December 2023).
2. Mujtaba B, Cavico F. E-commerce and social media policies in the digital age: Legal analysis and recommendations for management. *Journal of Entrepreneurship and Business Venturing* 2023; 3(1): 119–146. doi: 10.56536/jebv.v3i1.37
3. Westfall A. AI voice-cloning scams are on the rise, here's how you can protect yourself: Experts say the scams are disturbing but they work. Available online: https://www.foxbusiness.com/technology/ai-voice-cloning-scams-rise-heres-how-protect-yourself (accessed on 18 December 2023).
4. Australian Cyber Security Centre. *ACSC Threat Report*. Australian Cyber Security Centre; 2016.
5. Payne BK. Defining cybercrime. In: Holt TJ, Bossler AM (editors). *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Springer International Publishing; 2020. pp. 3–25.
6. Aggarwal P, Arora P, Ghai R. Review on cyber crime and security. *International Journal of Research in Engineering and Applied Sciences* 2014; 2(1): 48–51.
7. Buil-Gil D, Miró-Llinares F, Moneva A, et al. Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies* 2020; 23(sup1): S47–S59. doi: 10.1080/14616696.2020.1804973
8. Finklea K, Theohary CA. *Cybercrime: Conceptual Issues for Congress and US Law Enforcement*. Congressional Research Service, Library of Congress; 2015. pp. 214–226.
9. Friend C, Grieve LB, Kavanagh J, Palace M. Fighting cybercrime: A review of the Irish experience. *International Journal of Cyber Criminology* 2020; 14(2): 383–399. doi: 10.5281/zenodo.4766528
10. Holt TJ. Regulating cybercrime through law enforcement and industry mechanisms. *The ANNALS of the American Academy of Political and Social Science* 2018; 679(1): 140–157. doi: 10.1177/0002716218783679
11. Taylor RW, Fritsch E, Liederbach J, et al. *Cyber Crime and Cyber Terrorism*, 4th ed. Pearson; 2018. 464p.
12. The Law Office of Elliott Kanter. Defending against cybercrime charges in California. Available online: https://www.enkanter.com/article/defending-against-cyber-crime-charges-in-california (accessed on 18 December 2023).
13. U.S. Attorney's Office. Brooklyn Man pleads guilty and is sentenced for hacking into online accounts of wegmans customers. Available online: https://www.justice.gov/usao-wdny/pr/brooklyn-man-pleads-guilty-and-sentenced-hacking-online-accounts-wegmans-customers (accessed on 18 December 2023).
14. Kort A. Dar al-Cyber Islam: Women, domestic violence, and the Islamic reformation on the World Wide Web. *Journal of Muslim Minority Affairs* 2005; 25(3): 363–383. doi: 10.1080/13602000500408393
15. Phillips K, Davidson JC, Farr RR, et al. Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences* 2022; 2(2): 379–398. doi: 10.3390/forensicsci2020028
16. AlMatrooshi AM, Gilani SR, Mujtaba BG. Assessment of mandatory reporting laws to break the silence of child sexual abuse: A case study in the United Arab Emirates. *SN Social Sciences* 2021; 1(8): 209. doi: 10.1007/s43545-021-00216-4
17. Lallie HS, Shepherd LA, Nurse JR, et al. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security* 2021; 105: 102248. doi: 10.1016/j.cose.2021.102248
18. Lusthaus J, Bruce M, Phair N. Mapping the geography of cybercrime: A review of indices of digital offending by country. In: Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW); 7–11 September 2020; Genoa, Italy. doi: 10.1109/EuroSPW51379.2020.00066
19. McGuire M, Dowling S. *Cyber Crime: A Review of The Evidence*: *Summary of Key Findings and Implications: Home Office Research Report 75*. Home Office; 2013.
20. Monteith S, Bauer M, Alda M, et al. Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports* 2021; 23: 18. doi: 10.1007/s11920-021-01228-w
21. Radoniewicz F. International regulations of cybersecurity. In: Chałubińska-Jentkiewicz K, Radoniewicz F, Zieliński T (editors). *Cybersecurity in Poland*. Springer; 2022. pp. 165–179. doi: 10.1007/978-3-030-78551-2_5
22. Rani S, Kataria A, Sharma V, et al. Threats and corrective measures for IoT security with observance of cybercrime: A survey. *Wireless Communications and Mobile Computing* 2021; 2021: 579148. doi: 10.1155/2021/5579148
23. Reep-van den Bergh CMM, Junger M. Victims of cybercrime in Europe: A review of victim surveys. *Crime Science* 2018; 7(1): 5. doi: 10.1186/s40163-018-0079-3

24. Mujtaba BG. Cybercrimes and safety policies to protect data and organizations. *Journal of Crime and Criminal Behavior* 2024; in press.
25. Saini H, Rao YS, Panda TC. Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications* 2012; 2(2): 202–209.
26. Gilani SRS, Rehman HU, Khan I. The conceptual analysis of the doctrine of proportionality and, its role in democratic constitutionalism. *Journal of Education & Social Research* 2021; 4(1): 204–210. doi: 10.36902/sjesr-vol4-iss1-2021(204-210)
27. Mujtaba BG. Operational sustainability and digital leadership for cybercrime prevention. *International Journal of Internet and Distributed Systems* 2023; 5(2): 19–40. doi: 10.4236/ijids.2023.52002
28. Gilani SR, Khan I, Zahoor S. The historical origins of the proportionality doctrine as a tool of judicial review: A critical analysis. *Research Journal of Social Sciences and Economics Review* 2021; 2(1): 251–258. doi: 10.36902/rjsser-vol2-iss1-2021(251-258)
29. Mujtaba BG. Ethical implications of employee monitoring: What leaders should consider. *Journal of Applied Management and Entrepreneurship* 2003; 8(3): 22–47.
30. Gilani SRS. *The Significance of the Doctrine of Proportionality in the Context of Militant Democracy to Protect the Freedom of Expression* [PhD thesis]. Brunel University London; 2019.
31. Cavico F, Mujtaba B, Lawrence E, Muffler S. Examining the efficacy of the common law tort of intentional infliction of emotional distress and bullying in the context of the employment relationship. *Business Ethics and Leadership* 2018; 2(2): 14–31. doi: 10.21272/bel.2(2).14-31.2018
32. Buil-Gil D, Miró-Llinares F, Moneva A, et al. Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies* 2021; 23(S1): S47–S59. doi: 10.1080/14616696.2020.1804973
33. Aggarwal G. General awareness of cyber crime. Available online: https://www.semanticscholar.org/paper/General-Awareness-on-Cyber-Crime-Aggarwal/040b800a8a68bc1eb48ca8a655294e61e088b4af (accessed on 21 December 2023).
34. Peelen AAE, van de Weijer SGA, van den Berg CJW, Leukfeldt ER. Employment opportunities for applicants with cybercrime records: A field experiment. *Social Science Computer Review* 2023; 41(5): 1562–1580. doi: 10.1177/08944393221085706