Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4, 2072-2093
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i4.1583

An in-depth PRISMA based review of cybercrime in a developing economy: Examining sector-wide impacts, legal frameworks, and emerging trends in the digital era

Md Noor Uddin Milon[1], Provakar Ghose[2], Tania Chowdhury Pinky[3], Mst. Nowshin Tabassum[4], Md Nazmul Hasan[5], Maimuna Khatun[1*]
[1]Government of people's Republic of Bangladesh, National Board of Revenue, Dhaka-1000, Dhaka, Bangladesh; noor.milon414@gmail.com (M.N.U.M.)
[2]MS in Business Analytics, University of New Haven, West Haven, United States; pghos1@unh.newhaven.edu (P.G.)
[3,4]Department of Management Information Systems, Faculty of Business Studies, Begum Rokeya University, Rangpur, Rangpur-5404, Rangpur, Bangladesh; rashedachowdhury641@gmail.com (T.C.P.) nowshin.mouly@gmail.com (M.N.T.)
[5]MS in Business Analytics, University of New Haven, West Haven, Connecticut, United States; mhasa9@unh.newhaven.edu (M.N.H.)
[1]Department of Management Information Systems, Faculty of Business Studies, Begum Rokeya University, Rangpur, Rangpur-5404, Rangpur, Bangladesh; khatunmaimuna987@gmail.com (M.K.).

Abstract: In today's digital age, the swift advancement of information and communication technology (ICT) has brought immense benefits to humanity, but it has also opened the door to various technological crimes, particularly cybercrime, which is becoming an increasingly significant issue in Bangladesh. This paper aspires to critically examine the nature and scope of cybercrime in Bangladesh, exploring its impact on individuals, businesses, and the economy as a whole. This study investigates the state of cybercrime in Bangladesh, its sector-wide impacts, and the effectiveness of existing legal government law in combating these crimes. a survey alongside semi-structured interviews and a variety of sources, including Scopus, Web of Science, DOAJ, Scimago, and Google Scholar databases. The study also utilized PRISMA based methodology to find out the research gaps in the context to increase deeper insights and understanding into technology-related crimes. Cybercrime (hacking, phishing and credit Card Fraud, financial fraud etc) greatly affected economic growth, emerging trends, different sectors, banking, finance and legal frameworks which are emerging economies that have the mediation process of expanding factors in Bangladesh. Additionally, financially motivated attackers, politically motivated attackers and espionage motivated attackers are the main reasons for cybercrime. As Bangladesh rapidly adopts digital technologies, the study identifies the emerging factors, patterns, underlying logic, the role of law enforcement agencies and cybersecurity measures related to cybercrime. The implication will be presented in the increasingly alarming consequences of cybercrime and suggests strengthening existing global cyber laws to more effectively fight these crimes.

Keywords: *Cyber appellate tribunal, Cyber tribunal, Cybercrime, Cybersecurity, Digital era, Emerging trends, Legal framework, Sectoral impact*

1. Introduction

Bangladesh is experiencing a significant transformation across various sectors, including commerce, finance, and social communication, driven by the widespread adoption of the internet and smartphones (Gadallah et al., 2024). This surge in digital connectivity has fueled substantial economic growth and enhanced social interaction, positioning Bangladesh as a key player in the global digital arena (Lucila et al., 2024). However, alongside these opportunities, the country is also confronting a rising number of

* Correspondence: khatunmaimuna987@gmail.com

cyber threats that pose risks to its economic stability, national security, and social fabric (Radanliev, 2024).

Cybercrime has become a significant threat in Bangladesh, manifesting in various forms such as identity theft, online fraud and harassment. These criminal activities not only target individuals but also put critical infrastructures like financial institutions, government agencies and telecommunication networks at risk (Meng & Li, 2023). Although legislation such as the Telecommunication Regulation Act of 2001, the ICT act 2006 and the Digital Security Act of 2018 has been enacted, the country's cyber defenses remain insufficient, often lagging behind the increasingly sophisticated and evolving nature of cybercrime (Heffernan et al., 2020).

Again, Heffernam et al. (2020) demonstrate that the economic impact of cybercrime in Bangladesh is alarming. A significant lack of consumer trust heavily affects those e-commerce sectors which is vital to the country's digital economy. Research indicates that consumer hesitation to participate in online activities is often driven by fears of cybercrime and perceived deficiency in cybersecurity measures. Additionally, the shortage of cybersecurity expertise and resources within many businesses increases their susceptibility to attacks further undermining consumer confidence and economic progress.

Venkatachary et al. (2024) suggest that tackling these challenges necessitates a comprehensive and multifaceted approach. This approach focuses on enhancing cybersecurity frameworks, bolstering technical resilience and rebuilding consumer thrust. Key steps include investing in cybersecurity infrastructure, establishing specialized teams like computer emergency Response Teams and implementing robust cyber defense strategies. Additionally, it is crucial to educate stakeholders about cybersecurity best practice and the importance of strong defenses mechanisms to create a secure digital environment (Joshi et al., 2023).

Achaal et al. (2024) believe that This study aims to explore the diverse nature of cybercrime in Bangladesh, critically assessing the effectiveness of current regulatory frameworks and identifying gaps that hinder the country's efforts to achieve robust cybersecurity. By examining the socio-technical context and legislative responses (Achaal et al., 2024), the research seeks to enhance understanding of the challenges and potential solutions for bolstering national cyber resilience. Additionally, the study will investigate the relationship between cybersecurity, consumer trust and secure its digital future (Priom et al., 2024). This thorough analysis intends to contribute to the development of a strong cybersecurity framework that supports Bangladesh's digital transformation while safeguarding its economic and social interests (Heffernan et al., 2020).

According to Prasetyo et al. (2024), Public, private, or nonprofit organizations did not specifically fund this research. One of the biggest problems in cybersecurity is protecting sensitive user information, like passwords and PIN codes. Billions of users unwittingly provide sensitive information on phony login pages every day. Cyberattack techniques that are frequently employed to entice users to compromised websites include phishing, captivating advertisements, click-jacking, malware, SQL injection, session hijacking, man-in-the-middle, denial of service, and cross-site scripting.

2. Research Gap

There are accuracy and latency issues with these techniques on cybercrime. Including all citizens in the fight against threats is a key component of a whole-of-state cybersecurity strategy (Prasetyo et al., 2024). Notwithstanding, inadequate data regarding citizens' level of protection may impede agencies' capacity to comprehend the issue completely and offer practical recommendations for mitigating cyber threats. For science, information, and communication technology to advance, the telecommunications sector must expand. However, a lack of deregulation and open competition has left this industry underdeveloped (Ilushin & D, 2024). According to Shao (2022), As internet financial transactions are still relatively new, Bangladesh is not particularly concerned about the effects of cybercrime at this time. However, the prevalence of computer crimes could rise sharply if the government does not make the necessary investments in the infrastructure and technology to stop, identify, and prosecute these crimes

as online financial transactions become more widespread. These are risky and lucrative endeavors for cybercriminals.

3. Research Objectives

RO1: To investigate the current condition and consider its effect of cybercrime on various sectors in a developing economy like Bangladesh.

RO2: To assess the prevalence of cybercrime in an emerging economy and evaluate the effectiveness of existing laws and regulations in addressing these crimes.

4. Literature Review

4.1. Cybercrime in Bangladesh

Pal (2022) points out Cybercrime encompasses a variety of illegal activities where traditional crime is adapted to involve computers, either as the target or the means of the criminal activity. This term applies to any offense that involves electronic communication or information systems, including the use of devices, the Internet, or any combination of these. Cybercrime refers to a broad spectrum of criminal acts, ranging from hacking to denial-of-service attacks, where computers or networks serve as tools, targets, or environments for illegal activities. It also includes conventional crimes that are facilitated by the use of computers or networks (Gadallah et al., 2024). According to Ali (2019), Cybercrime refers to illegal activities conducted online or through computer networks. In recent years, the Internet has become an essential tool for connecting people globally, offering numerous benefits and opportunities through the widespread sharing of important information. However, the growing number of Internet users has also led to the serious issue of cyber-attacks. Kadeni (2023) shows that in Bangladesh, a district judge has highlighted several common forms of cybercrime in the country, such as sending harmful emails to VIPs and foreign diplomatic missions, distributing pornography, using email for illegal activities, spreading malicious and false information online, and facilitating prostitution through online platforms. Cybercrimes can take many different forms, such as denial-of-service assaults, virus attacks, online abuse like cyberbullying, email scams or phishing, and identity theft. Child pornography, the solicitation and production of child pornography, the propagation of hate speech or the encouragement of terrorism, grooming, copyright violations, and the selling of illicit goods are some more instances (Anzelone & Katz, 2024). Forgery, including the production of phony documents or certifications, deceptive advertising, ransomware attacks, spamming, botnets, and phony bank warnings or unwanted SMS messages asking private information like a Bank Verification Number (BVN), can also be included in cybercrimes (Rickards, 2023).

4.2. Cybercrime and its Negative Effects in Bangladesh

According to Petersen et al. (2023), Cybercrime has significant and wide-ranging impacts on society. For instance, activities such as online pornography and prostitution erode societal morals and increase the likelihood of a decline in ethical standards and norms. Additionally, cybercrime can harm a country's socioeconomic well-being by lowering productivity levels. Moreover, countries with high rates of cybercrime often face distrust in online transactions (Choi et al., 2023). However, due to proactive management, approximately 42% of businesses initially affected by cybercrime have either recovered well or experienced an increase in revenue. Cybercrime is on the rise in Bangladesh due to several factors, including the country's growing unemployment rate and the increasing availability of affordable internet services (Kundu & Plambeck, 2024). More broadly, data shows that 39% of cyber fraud is caused by external factors, such as customers (26%), hackers (24%), and vendors or third parties (19%). Internal perpetrators account for another 39%, including middle management (34%), operational staff (31%), and senior management (26%). Additionally, 20% of cyber fraud cases involve collusion between external and internal actors. Vaishy and Gupta (2021) concern that as international relations and economic, financial, cultural, social, and governmental exchanges increasingly take place online, cybercriminals have begun targeting government agencies and private businesses as well.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

4.3. The Internet Affects the Rate of Cybercrime in Bangladesh

Chamakiotis et al. (2024) conducted a study that Technology has become indispensable in our daily lives, evolving into one of the most essential needs for everyone in today's world. It is now so deeply embedded in our routines that imagining life without it seems almost impossible. Technology influences nearly every aspect of our lives, including education, work, communication, reflection, and learning. According to a study conducted in Bangladesh (Spence & Clapton, 2018), males are more active on the internet (31.58%) compared to females (21.74%). This disparity could be due to men having a greater interest in exploring new technologies or unknown territories, or it may be that men are more attracted to potentially addictive activities like pornography, cybersex, and online gaming. Technological vulnerabilities can sometimes serve as entry points for cyberattacks. Security experts around the world have raised concerns about the insufficient protective measures in Internet of Things (IoT) devices, regardless of their type or connectivity method. Most consumers tend to prioritize IoT devices that are user-friendly and enhance their daily lives. The telecommunications sector within the network industries provides services such as voice and data transmission, internet access, and both fixed and mobile phone services (Bhuiyan et al., 2024). The network industries also encompass sectors like information technology, including software and hardware, as well as multimedia industries such as broadcasting, cable television, and companies involved in delivery services (Gökdemir, 2021). A study found that the majority of internet users in Bangladesh prefer social media platforms, with 35.2% spending more than three hours per day on these sites (Buettner et al., 2020). The internet serves a variety of purposes depending on user needs, including browsing, research, education, communication, and financial transactions. In today's world, engaging in illegal activities online has become increasingly lucrative and secure. Cybercrime, also known as e-crime or electronic crime, involves the use of computers and communication devices for criminal activities (Kikerpill, 2023). Van (2023) report that the incidence of e-crimes has surged significantly, impacting businesses, government agencies, society, and individuals at large. Researchers have proposed several theories to explain the motivations behind hacker and cybercriminal activities, suggesting factors such as financial gain, personal revenge, and the lack of stringent cybercrime laws and regulations.

4.3. Cybercrime of Generation Z in Bangladesh

Evans (2023) expresses that Generation Z transitions into adulthood, they are expected to bring about a significant shift in both social and economic aspects. The future colleagues of millennials will largely be from Generation Z. Despite sharing many superficial traits with millennials, Generation Z appears to differ markedly in their approach to privacy. While Generation Z often approaches cybersecurity responsibilities with less preparedness, millennials benefit from the collective skills and knowledge of Generation Z. Literature on Generation Z indicates that they seek a smooth entry into the professional world. Generation Z is recognized as one of the most sophisticated and intelligent cohorts to date (Molla et al., 2023). According to Chandra and Singh (2024), Many young people in this generation view self-employment as a desirable career path, valuing its potential for profitability and the autonomy it offers. Generation Z is also known for its willingness to take risks and succumb to peer pressure (Bhuiyan et al., 2024). Raised in the era of social media and the internet, they are among the most technologically adept generations. However, since some members of this generation are still in their early career stages and others have yet to enter the workforce, there is limited scholarly discussion about their professional characteristics.

4.4. Bangladesh and Law Against Cybercrime

Tadi (2023) conducted a study that there is a call to shift from "digital optimism" to "digital pragmatism," advocating for technologies to be "secured by design" as a strategy to combat cybercrime and enhance trust and adoption of new technologies. Recognizing the threat posed by cybercriminals, the Bangladeshi government has enacted legislation to address this issue in the context of the digital age and economy. The Digital Security Act, 2018 has been introduced to tackle the challenges

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

associated with cybercrime and digital security. This act is part of a broader regulatory framework concerning information technology (Kalėda, 2023). Cybersecurity involves safeguarding electronic devices, networks, systems, and related infrastructure from malicious data attacks and other threats (Mani, 2024). It is a crucial concern for all users of electronic devices, including businesses, governments, and individuals. Akter and Bhuiyan (2024) emphasizes that the primary objective of cybersecurity is to minimize the risk of harmful attacks on computers, software, and networks. This field employs various tools to detect intrusions, prevent infections, block unauthorized access, enforce authentication, enable encrypted communication, and perform many other protective functions.

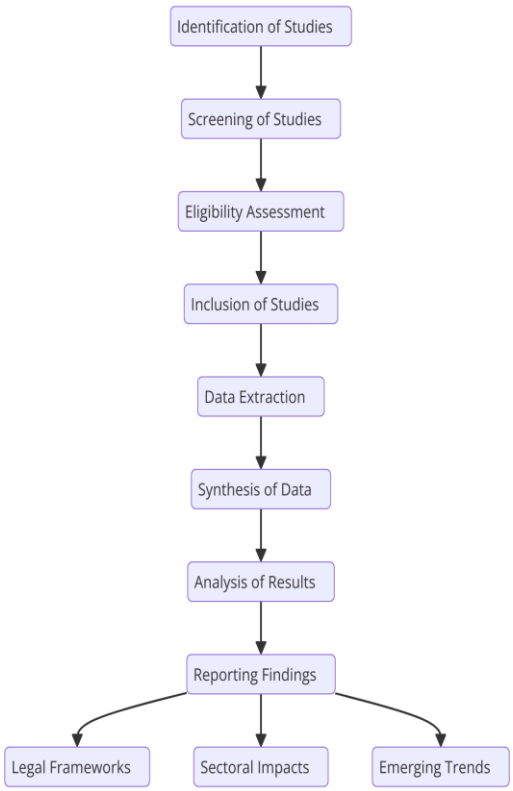

Figure 1.
A systematic PRISMA based methodology.

5. Methodology

Researcher used previous studies to conduct this research where an explanation of each step in the PRISMA-based research methodology is discussed to present scenario for evaluating the impact of cybercrime in developing economies: Duckert and Barkhuus (2022) analyzes that this study used a qualitative research approach to gather in-depth information regarding the awareness of Bangladeshi population in Figure 1. Additionally, secondary data were collected through an extensive review of existing literature (Kluener et al., 2024). Utilizing books by renowned authors, credible journal articles, research reports, and articles from reputable media and websites can influence the pace of Bangladesh's adoption of cyber legislation by means of PRISMA based methodology (Kaium et al.,2019). The literature review encompassed both recent and historical studies sourced from databases such as Scopus, Web of Science, DOAJ, Scimago, and Google Scholar which is presented in Figure 1.
The following steps are conducted to determine the systematic methodology.

5.1. Identification of Studies

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

The first step involves identifying relevant studies, articles, reports, and other literature that discusses the impact of cybercrime on developing economies in Figure 1. This typically involves searching various databases and sources to gather as much relevant information as possible (Barnor & Patterson, 2020).

5.2. Screening of Studies

After identifying the studies, the next step is to screen them to remove duplicates and irrelevant studies. This step ensures that only those studies that meet the predefined criteria move forward in the process (Lizunov et al., 2021).

5.3. Eligibility Assessment

In this step, the remaining studies are further assessed based on their eligibility. This involves a detailed review of the content to ensure that the studies directly address the research questions or objectives. Studies that do not meet the eligibility criteria are excluded (Bhuiyan et al., 2024).

5.4. Inclusion of Studies

According to Barnor & Patterson (2020), the studies that pass the eligibility assessment are included in the final review in Figure 1. These are the studies that will be analyzed in detail to understand the impact of cybercrime on developing economies.

5.5. Data Extraction

In this step, data is systematically extracted from the included studies. The extracted data typically includes key information such as study characteristics, outcomes, and findings related to cybercrime's impact (Islam et al., 2024).

5.6. Synthesis of Data

The extracted data is then synthesized to provide a comprehensive overview of the research findings. This synthesis may involve combining data from multiple studies to identify patterns, trends, and common themes.

5.7. Analysis of Results

Saxena (2023) the synthesized data is analyzed to draw conclusions about the impact of cybercrime on developing economies. This step involves interpreting the data to understand the broader implications and significance of the findings in Figure 1.

5.8. Reporting Findings

The final step involves reporting the findings of the research. This typically includes writing a detailed report or paper that outlines the impact of cybercrime, the effectiveness of legal frameworks, the sectoral impacts, and emerging trends in the digital age in the Figure 1 (Jadhav, 2024).

5.9. Legal Frameworks

Widodo et al. (2024) within the reporting, specific attention is given to the analysis of existing legal frameworks in developing economies and their effectiveness in combating cybercrime.

5.10. Sectoral Impacts

The report also examines how different sectors, such as finance, healthcare, and government, are impacted by cybercrime (Levin, 2023).

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

5.11. Emerging Trends

Finally, the report identifies and discusses emerging trends in cybercrime and digital security within developing economies (Meah, & Hossain, 2023). This can include new types of cyber threats, changes in cybercriminal behavior, and innovations in cybersecurity measures (Bhuiyan, 2024). This structured approach ensures that the research is thorough, systematic, and based on a comprehensive analysis of existing literature, providing valuable insights into the complex issue of cybercrime in developing economies (Ciuchi, 2022).

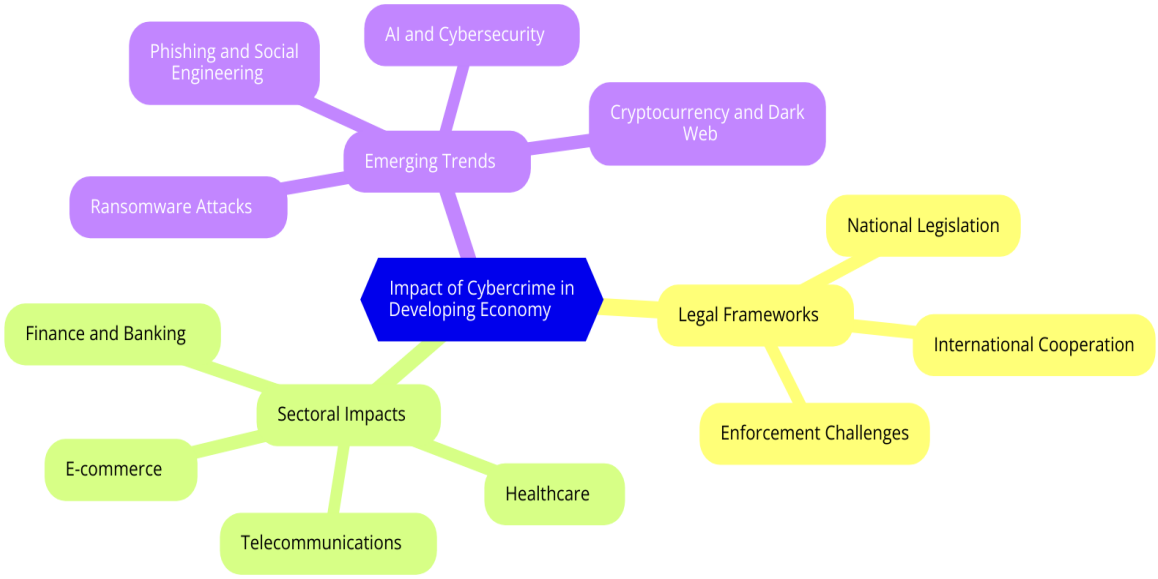

Figure 2.
Impact of cybercrime in emerging economy over the world.

6. Discussion

6.1. Impact of Cybercrime in Emerging Economy

Leukfeldt and Kleemans (2019) display that cybercrime is characterized as computer-mediated activities deemed illegal or criminal by specific authorities, occurring within global economic networks. This concept indicates that cybercrime operates in a digital environment, where information about individuals, items, events, or facts is mathematically encoded and transmitted through local and global networks. According to Figure 2, cybercrime significantly impacts the economy by affecting economic development, driving emerging trends, influencing various sectors, and interacting with interconnected legal frameworks (Ukwuoma, 2021). These ideas are further expanded by considering the multiple sectors in emerging economies that are impacted by the cybercrime mediation process (Wall, 2017).

Sectoral impact: Figure 2 presents that the sectoral impact is interconnected by the crucial sector of the world. Without these sectors, the emerging economy is in a deadlock that is directly engaged. As these sectors are necessary for an emerging economy (Cruz, 2023).

Finance and Banking: Cybercrime poses a significant threat, encompassing a broad range of online criminal activities across various contexts. In the twenty-first century, financial institutions have been especially alarmed by the swift increase in cybercrime (Bhuiyan et al., 2024). Over the years, the impact of these attacks on financial institutions has been closely examined and compared (Oreku, 2021).

E-commerce: Establishing consumer trust and upholding robust cybersecurity practices are essential for the sustained growth of e-commerce. The rise of e-commerce has significantly transformed the way business and customers interact (Adakawa, 2023).

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

Telecommunication: The telecommunications industry is a prime target for cybercriminals. This sector includes a diverse array of businesses, ranging from internet service providers to telephone, mobile, and satellite companies, among others. Its expansive reach enables cybercriminals to launch large-scale attacks affecting a broad spectrum of customers and organizations (Miftari et al., 2022).

Healthcare: Cybercrime greatly impacts the healthcare sector, with the main challenges targeting key operators and users of technology. Beyond investing in IT infrastructure, it is crucial to enhance healthcare workers' awareness and encourage them to actively protect patient data. Education and training play a vital role in achieving this (Aldawood & Skinner, 2019).

Legal framework: Current legal frameworks can manage threats at a national level, but regional digital dangers often fall outside the scope of broader cyber laws, leading to insufficient global responses to increasing cybercrimes. Moreover, achieving global consensus and agreement may complicate addressing cybersecurity as an international issue. These legal shortcomings stem from policy approaches that could potentially lead to innovative solutions for the complex nature of digital threats (Abthal & Tarik, 2024).

National legislation: Cybercrime legislation offers a broad framework of rules and regulations. Among these, some are global in scope and address a wide array of dangerous online activities. This legislation includes provisions for the evolving nature of crime as technology advances and addresses acts of terrorism conducted through cybercrime, such as theft of financial assets from banks (Bhuiyan & Akter, 2024).

International cooperation: Collaboration can result in the development of universally accepted rules and regulations for cyber activities, streamlining legal procedures and enhancing consistency in the global fight against cybercrime (Kabir et al., 2024). This standardization is essential for ensuring a coordinated international response and preventing hackers from taking advantage of legal differences between jurisdictions.

Enforcement challenges: This study identified operational enforcement challenges, particularly resource constraints and issues with managing digital evidence (Bhuiyan et al., 2024). Our observations regarding legal ambiguity align with the recognized problems in implementing cybercrime laws and policies, highlighting the critical issue of unclear legislation that hinders the prosecution and adjudication of cyber offenses.

Emerging trends: Examining Figure 2 reveals the importance of recognizing prevalent trends and strategies employed by hackers. By examining these tactics, researchers can gain insights into how cybercriminals evolve with technological advancements and exploit weakness in digital systems. Grasping these core patterns and methods is crucial for understanding the evolving nature of digital threats (Amin et al., 2024).

AI and cyber security: Integrating AI technology into cybersecurity operations requires a careful equilibrium between automation and human oversight. This balance is essential for fully leveraging AI's capabilities while mitigating the risk of unintended consequences from automated systems. Effective collaboration between humans and machines ensures that AI tools support rather than replace the decision-making skills of cybersecurity experts (Koen, 2020). As depicted in Figure 2, human supervision is necessary to interpret and contextualize AI-generated alerts, which might otherwise lead to false positives or miss critical subtleties in cyber threats.

Phishing social Engineering: Phishing continues to be a prevalent tactic used by cybercriminals to deceive individuals and organizations. These attacks often involve fraudulent emails, text messages or websites designed to trick victims into revealing personal details like login credentials or financial information (Poli et al., 2024). Phishing schemes are growing more advanced, employing social engineering methods to manipulate human behavior and bypass security measures.

Ransomware Attacks: As illustrated in Figure 2, ransomware affects all types of businesses, but it is particularly effective against targets in the government, aviation, and aerospace sectors. These attacks are increasingly sophisticated and widespread, making it challenging to keep pace with the growing body of documentation on this malicious software.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

Cryptocurrency and dark web: At present, the dark web and cryptocurrency assets are significant sources of anonymous activity, with the Tor browser readily accessible for download online. This anonymity raises growing concerns among the public about safeguarding personal information and financial assets in the digital realm. However, law enforcement agencies work to mitigate the risks to global economic systems and address the humanitarian impacts associated with these hidden services.

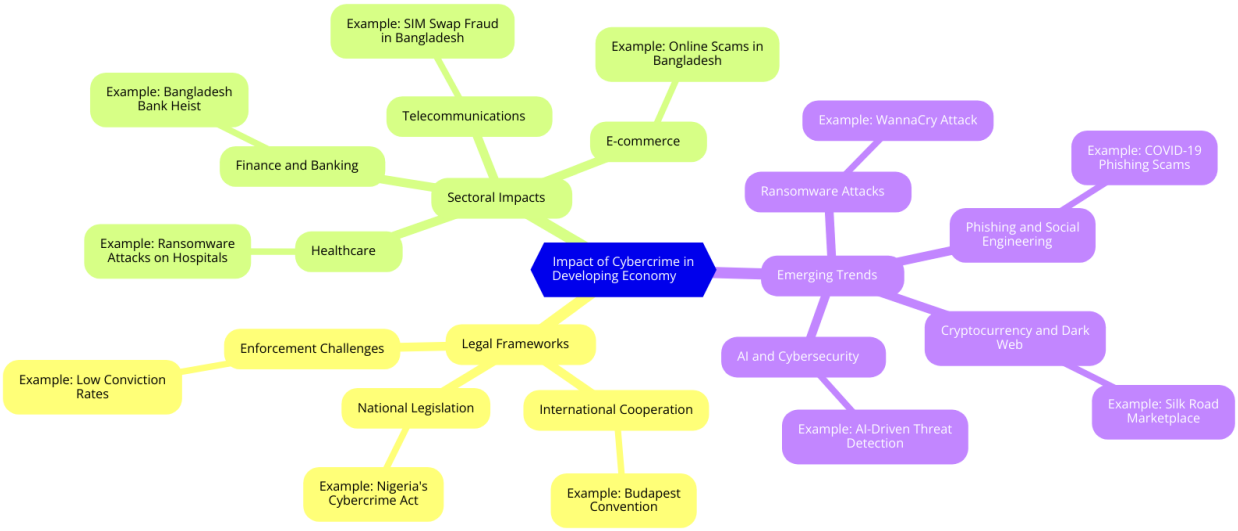

Figure 3.
Example of cybercrime in Bangladesh perspective.

One of the most infamous cybercrimes in Bangladesh was the 2016 Bangladesh Bank Heist, where hackers managed to steal $81 million from the central bank's account at the Federal Reserve Bank of New York (The Daily Star, 2016). The heist was carried out by sending fraudulent transfer requests via the SWIFT payment system. This incident highlighted significant vulnerabilities in financial systems and led to increased scrutiny and reforms in banking security measures by Figure 3 across the country.

SIM swap fraud is a type of identity theft where criminals use social engineering techniques to convince mobile service providers to transfer a victim's phone number to a new SIM card. In Bangladesh, this type of fraud has been used to gain access to victims' bank accounts and other sensitive information (Siregar, 2020). This has led to financial losses and compromised personal information, prompting telecom companies to enhance their verification processes (Maria, 2024).

Figure 3 demonstrates e-commerce which has grown in Bangladesh, so have online scams. Fraudulent websites and sellers exploit consumers by offering fake products or never delivering the purchased goods. Common scams include counterfeit goods, phishing sites that steal payment information, and fraudulent online stores. These scams undermine consumer confidence in online shopping and have resulted in financial losses for many individuals (Saha et al., 2024).

Bangladesh has undergone a significant technological transformation. The adoption of information and communication technologies (ICT) has dramatically changed modern life, providing access to a wide range of advanced services, real-time communication, and nearly limitless information. However, as reliance on technology increases, so does the risk of its misuse, leading to greater vulnerability. This shift has also led to a concerning rise in the number and scale of cybercriminals, along with the widespread availability of malware and spyware online (Strader et al., 2024).

Cybercrime encompasses a wide range of illegal activities where a computer is either the tool or the target of the crime. According to the Information Technology Act, it involves any unlawful actions carried out through or on computers, the internet, or other digital technologies (Alexandrou, 2021). Amin et al. (2024) focus on these crimes which not only cause significant disruption to society and

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

government but also allow perpetrators to conceal their identities. Technologically skilled criminals leverage the internet to commit various illegal acts. Broadly speaking, cybercrime can be defined as any illegal activity where a computer, the internet, or both are used as tools, targets, or in some cases, both.

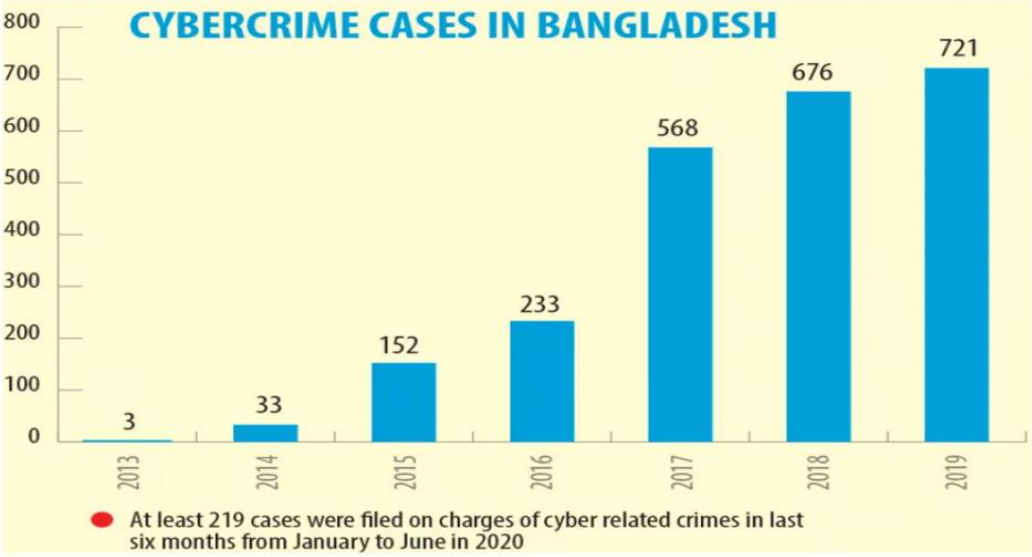

Figure 4.
Cybercrime cases in Bangladesh.

Figure 4 is found that Cybercrimes in Bangladesh currently include life-threatening emails sent to prominent individuals, hostile emails to foreign diplomatic missions, attempts to extort money through fake emails, and the introduction of pornographic content on well-known websites. According to Kirtz (2018), Hacking has become a major concern in the country, with an increasing number of young people being drawn to the thrill of hacking. This trend extends beyond just youth, as even mainstream media is involved in hacking activities and the disclosure of private information.

6.2. General Characteristics of Cybercrime

Table 1.
The characteristics of cybercrime.

Characteristics	Description
Hacking	Illegally accessing another person's or organization's computer system constitutes hacking. This act places the victim in a vulnerable position, as it risks exposing all private data stored within the system. Hacking is a criminal offense, and those caught face significant legal consequences (Zhuk, 2024).
E-mail bombing	Collier (2020) said that e-mail bombing involves sending a large number of emails to a victim, which can overwhelm their email account and cause it to crash. This malicious act is intentionally carried out to harass or torment the target.
Cyber-terrorism	This refers to the intentional attacks by subnational groups or covert agents on data, computer systems, software, and information, resulting in harm to non-combatant targets. Cybercriminals often target financial data, transportation, and telecommunications systems. As a result, it is possible to achieve significant impact or victory without resorting to

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

Characteristics	Description
	physical violence (Ramírez & Prada, 2024).
Phishing and credit card fraud	This method involves employing deceptive tactics to obtain private information from users of bank and financial institution accounts. If electronic transactions are not properly secured, hackers may access credit card details and use them fraudulently by posing as the legitimate cardholder (Zahra et al., 2023).
Trojan attacks	According to Her et al. (2021), Trojan Horse is a type of code fragment that remains hidden within a program and performs covert operations. It is commonly used to disguise a worm or virus and can appear as a security tool. For instance, a female film director in the US had a Trojan installed on her computer, which enabled the attackers to access her webcam and capture images of her in her underwear. The criminals then used these images to harass her.
Software and intellectual Property theft	This involves stealing genuine information while disseminating false information to obscure the truth. Often, "saved" patents need further work and research, making intellectual property a common target for theft. Cybercriminals frequently exploit the internet to steal copyrights, trademarks, computer service codes, and other forms of intellectual property. This practice is sometimes known as cyber-squatting (Bhuiyan & Akter, 2023).
Financial fraud	This category of crimes encompasses activities such as unauthorized withdrawals of credit card numbers, bank fraud, and fraudulent online purchases (Dewi et al., 2023).

6.2. The Impact of Cyber Crime in Bangladesh

Akter et al. (2023) alarms the study that in Bangladesh, the impact of cybercrime is unavoidable and significantly affects the victims and their families. Such incidents often deliver a severe blow not only to the individuals directly involved but also to their loved ones, frequently leaving them out of the support process. Often, people uncritically accept information encountered in online media. This lack of awareness, education, and vigilance leads to a flawed and inconsistent belief system among the public (Liu, 2023). As a result, when a photo of a young woman is posted online and is fueled by careless gossip, many internet users do not take the time to verify its authenticity or manipulation. Overall, cybercrime is evolving into a global issue that threatens the national security of any country, including Bangladesh. The problem is becoming increasingly alarming for Bangladesh, especially in the context of globalization (Bhuiyan et al., 2023).

As stated by Bhukta (2020) in Figure 5, the complexity of Bangladesh's existing anti-cybercrime laws has enabled fraudsters to exploit various legal loopholes, contributing to the proliferation of cybercrime. With reduced opportunities for traditional crime and law enforcement's strong focus on enforcing the law, cybercriminals have increasingly turned to the internet as a new avenue for expanding their illegal activities.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

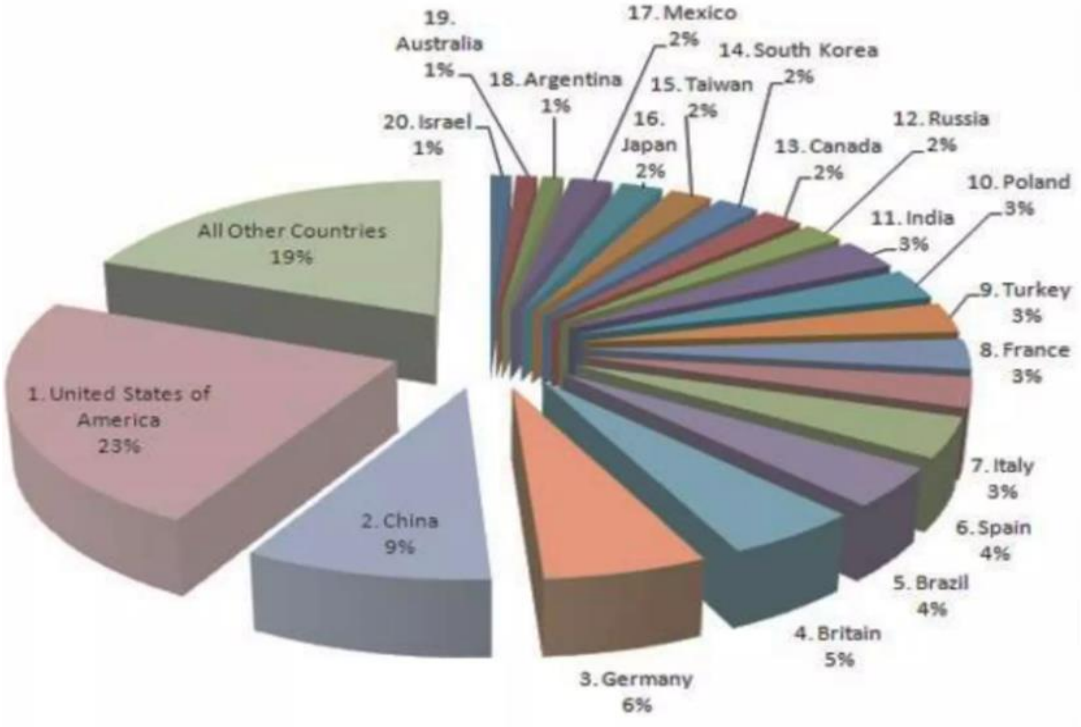

Figure 5.
Cybercrime top 20 countries.

Table 2.
Impact of cyber crime in Bangladesh.

Concept	Description	Reference
Cyber-crime and religion	The internet has driven a global digital transformation. While religious groups have effectively utilized online platforms for raising religious awareness, criminals have similarly adopted these platforms as venues for their illicit activities.	(Kim & Yong, 2024)
Economics and finance	Although cyberattacks have resulted in billions of dollars in losses for the banking sector, the impact of a major cyberattack in Bangladesh continues to be significant. Common targets for cybercriminals include stock exchanges, banks, and international financial transactions.	(Achaal et al., 2023)
Bangladeshi banks face cyber shadows	Cyberattacks have effects that extend beyond mere financial loss. They can disrupt entire economies, erode client trust, and damage reputations within the financial services sector. For instance, the Bangladesh Bank halted its internal online services in response to a potential cyberattack, highlighting the potential for widespread disruption and concern.	(Rahanaz et al., 2023)
Individuals	Email-based harassment is not a new phenomenon; it is similar to sending unwanted letters. In Bangladesh, there is no established national computer infrastructure or security system, and no dedicated oversight body has been created to address this issue.	(Bhardwaj, 2023; Sen et al., 2019)
	Cyberstalking involves monitoring an individual's online activities through various means, such as sending repeatedly offensive emails, posting threatening messages on the victim's frequently visited forums, joining the same chat rooms as the victim, and similar actions.	
	Online pornography can manifest in various ways, including hosting websites that contain such prohibited content, creating pornographic material on	

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

Concept	Description	Reference
	computers, and distributing or downloading this content through the Internet.	
	Online fraud and scamming have become highly lucrative and are rapidly growing in today's digital age. These fraudulent activities can take many forms, including credit card fraud, deceptive contracts, and misleading job offers, among others.	
Individuals property	Computer Vandalism: It refers to the deliberate destruction or damage of someone else's computer. This concept extends to any intentional physical harm inflicted on a computer, classifying it as vandalism.	(Arieska & Mukti, 202)
	Web Jacking: The term "hijacking" originates from this concept. These offenses allow a hacker to gain access to and control over another person's website, potentially leading to the alteration or destruction of the site's data.	
	Internet Time Thefts: These types of thefts generally lead to another person using the victim's internet browsing time. This is achieved by gaining access to the victim's login ID and password.	
	Intellectual Property Crimes / Distribution of Pirated Software: Intellectual property consists of a set of rights granted to the owner. An offense occurs when illegal actions fully or partially deprive the owner of these rights.	
Organizations	Unauthorized Control/ Access over Computer System: This practice is referred to as hacking.	(Corbet., 2022)
	Financial Institutions are at risk: Hackers pose a significant threat to financial institutions in Bangladesh. Although these institutions have implemented various online services, such as online banking and stock exchange transactions, they have not been able to ensure the highest level of security. Reports indicate that cybercriminal networks have targeted the country's technological infrastructure through the internet.	
The government	A specific form of crime within this category is cyberterrorism. The growth of the internet has revealed how individuals and organizations are using cyberspace to intimidate both domestic and international governments. When a person unlawfully accesses a military or government website, this activity constitutes terrorism. Reports indicate that the internet is increasingly being exploited by terrorist groups.	(Sharma, 2022)

According to Zhang et al. (2023), the study revealed that rumors are spread across seven areas on social media: entertainment, human rights, politics, health, education, and religion. Political rumors are particularly prevalent before and after elections. In contrast, the spread of false information related to religion has significantly increased in recent years. By 2020, religious rumors comprised 40% of the total rumors, up from just 5% in 2017.

Table 3.
Types of attacks.

The most common types of attacks	Percent	The most targeted of attacks	Percent
Phishing/Social Engineering	57%	Education/Research sector	75%
Compromised/Stolen devices	33%	Cyberattacks on the healthcare sector	71%
Credential theft	30%	ISP/MSP	67%
Government / Military sector	47%	Communications	51%

Source: Bhosale et al. (2021).

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

6.3. Reasons of Cybercrime in Bangladesh

Figure 6 presents that Cybercriminals now have easier access to sensitive information by exploiting vulnerabilities associated with our growing dependence on technology. Various cyber threats, including ransomware attacks and phishing emails, can severely undermine online privacy and security (Lanza et al., 2024). In accordance with Sharma (2022), these cybercrimes are caused by flaws or weaknesses in security systems. Some individuals do not prioritize security, neglecting to update their systems regularly. Cybercriminals can exploit these specific security gaps if operating systems or software are not consistently updated. Bangladesh experiences a range of cybercrimes that impact both individuals and society in Figure 6. There are numerous cases involving the theft of time and information online, vandalism of computer and network resources, intellectual property violations, forgeries, denial-of-service attacks, and the distribution of pornographic files (Verma, 2021).

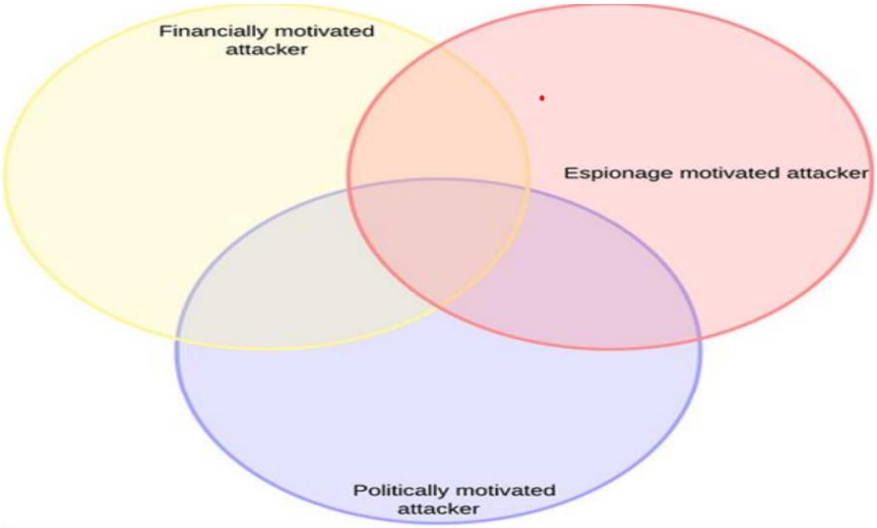

Figure 6.
Reasons of cyberattacks in Bangladesh.

6.4. Cyber Laws in Bangladesh

Saul and Heath (2021) display that cyberterrorism is a notable crime in this category. The growth of the internet has shown how individuals and organizations use cyberspace to intimidate both domestic and international governments. When someone illegally accesses a military or government website, it constitutes terrorism. Reports indicate that the internet is increasingly benefiting terrorist groups. Following Du (2023), the ICT Act, 2006 was enacted to foster the growth of information technology and support e-commerce. It includes provisions that could impose a penalty of up to ten years in prison, a fine of up to 10 million takas, or both. Recently, the Parliament updated the ICT Act 2006, instituting stricter penalties for cybercrimes.

6.5. The Cyber Security Act, 2023

The Digital Security Act has recently been enacted by Parliament as a replacement. It addresses some concerns raised about the previous law by reducing the maximum penalty for defamation and allowing bail for certain offenses (Bhuiyan et al., 2024). The Bangladeshi government is taking steps to combat the increasing threat of cybercrime (Lamé, 2019). However, there are still ongoing questions about the effectiveness and fairness of the country's cyber laws.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

Table 4.
Two types of cyber law.

Name of Laws	Description
Information and communication technology act, 2006	Section 3: Prohibits unauthorized access to data, devices, or computer systems.
	Section 4: Forbids altering or damaging a device, data, or computer system.
	Section 5: Prohibits the use of computers for committing fraud or creating forgeries.
	Section 6: Prohibits the use of computers to distribute pornographic content.
	Section 7: Forbids sending emails for commercial purposes without the recipient's consent.
The digital security act, 2018	Section 21: It has been noted that this section is quite broad and unclear that could harm the reputation of individuals or the state.
	Section 29: The use of computer systems to damage an individual's or organization's reputation is considered illegal. However, this provision has faced criticism for being vague and overly broad.
	Section 31: Grants police officers extensive authority to search and seize electronic devices without a warrant that has raised concerns about potential violations of privacy rights.
	Section 57: This provision has been contested on the grounds that it interfere with upon due to process rights and is perceived as unjust.

6.6. Cyber Tribunal

Section 68 of the Information and Communication Technology Act, 2006 mandates the establishment of one or more cyber tribunals by the government to address complaints under the Act efficiently within Figure 7 and Figure 8. In line with Dumberry (2018), The government will determine the jurisdiction of these tribunals, which will exclusively handle cases related to this Act. A Sessions Judge or Additional Sessions Judge, appointed in consultation with the Supreme Court, will preside over these tribunals (Hossain et al., 2024). Recently, the government has set up cyber tribunals in each of the eight regions of the country to adjudicate cases related to cybercrimes, including those under the Digital Security Act. Samarkina (2023) suggests by Figure 7 and 8 that Cyber Tribunal will follow the procedures outlined in the Criminal Procedure Code and will possess the same powers as a Sessions Court within its original jurisdiction. The public prosecutor will represent the government in these cases. The tribunal is required to complete the trial within six months from the date the charges are framed, with the possibility of a three-month extension. Additionally, the trial may be postponed for up to 10 days, but the tribunal must deliver its verdict within this extended timeframe.

From the perspective of Akter et al. (2023), the government plans to establish one or more online tribunals to handle complaints. Each appeal tribunal will consist of a chairman and two members appointed by the government. The chairman must be a sitting Supreme Court judge, a current judge eligible for Supreme Court appointment, or someone who qualifies for such a position. One of the two members must be a retired district judge or someone with legal experience, while the other must have extensive expertise in information and communication technology (Islam & Bhuiyan, 2022). The term of office for tribunal members will range from three to five years. Initially, the Cyber Appellate Tribunal will not have any authority. The Cyber Appellate Tribunal will review and decide on appeals from the orders and judgments of both the Cyber Tribunal and the Sessions Court only under appropriate circumstances. Kumar (2017) highlights that its decisions will be final, with the authority to modify,

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

amend, or overturn the original tribunal's rulings. The appellate tribunal will follow the appellate process of the Supreme Court's High Court Division (Rahman et al., 2024).

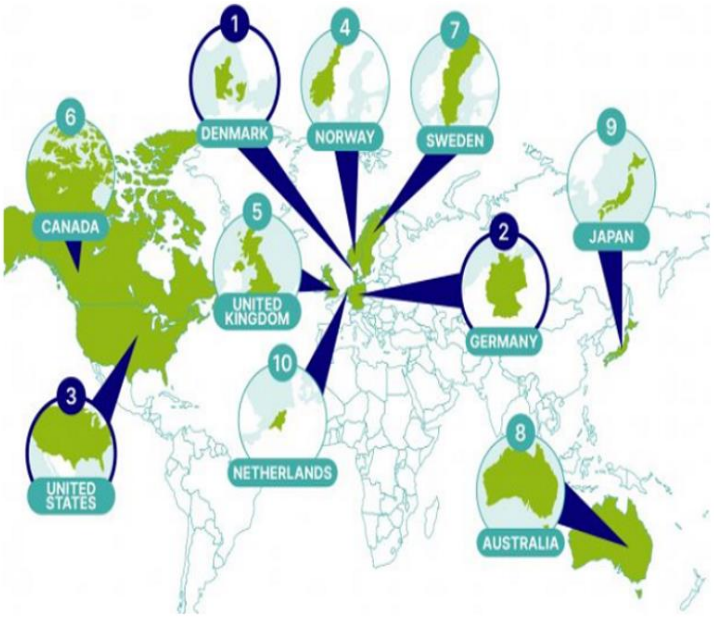

Figure 7.
The most low-risk countries for cyber threat.

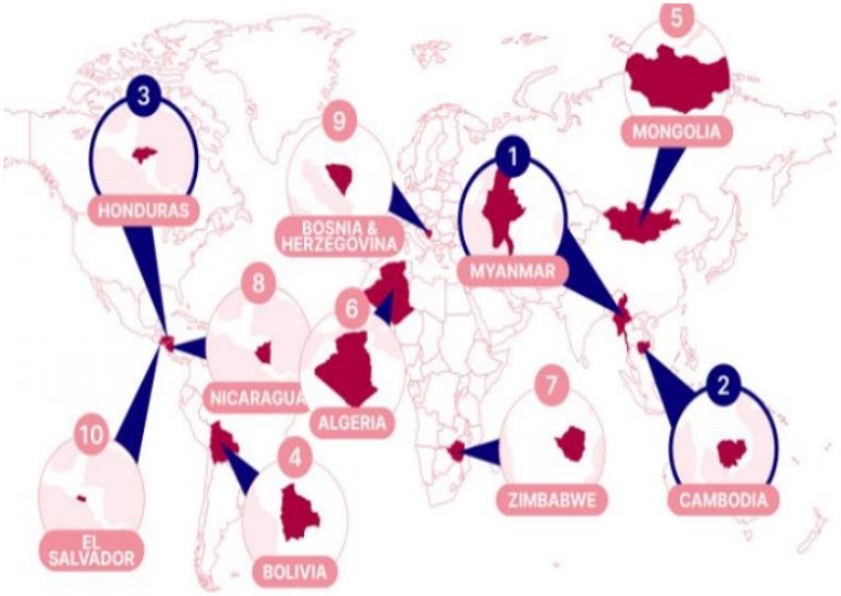

Figure 8.
The most high-risk countries for cyber threats.

7. Implication

Sleem & A (2022) describe that Bangladesh's cybersecurity environment is both complex and evolving, characterized by growing threats, regulatory challenges and technological advancements.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 2072-2093, 2024
DOI: 10.55214/25768484.v8i4.1583

Comprehending this landscape is essential for strategies to enhance and protect digital infrastructures, ultimately leading to a more secure Bangladesh. This section explores the key factors influencing the country's cybersecurity including the nature of threats, regulatory obstacles, technological process capacity building efforts, public awareness campaigns and technologies (Ebegba et al., 2022).

The article highlights the significance of cybersecurity for individuals, businesses, and the nation. It specifically looks at how perceived usefulness is while also considering the moderating effect of cyber legal implications on these relationships. The results offer fresh perspectives and deepen our understanding of behavior in Bangladesh. (Zhang, 2024).

8. Limitations and Future Research

Allowing the limitations of this study is essential. Relying on self-reported data may introduce as individuals might not accurately remember or disclose their experiences and behaviors. Factors such as rapid population growth, urbanization, unemployment, income inequality, and economic systems all play a role in the increasing cybercrime in Bangladesh. (Hillebrand & Hornuf, 2020).

Wang and Li (2024) highlighted the importance of enhancing generalizability in research. Longitudinal studies could offer valuable insights into how public perceptions of internet privacy evolve over time. The existing gap increases the country's susceptibility to sophisticated cyberattacks. To address this issue, Bangladesh must develop a comprehensive workforce development plan, expand educational opportunities, and increase public awareness about cybersecurity. Implementing these measures would strengthen the nation's cybersecurity infrastructure and secure its digital future. Additionally, cybercrime is a global challenge that often puts the efficacy of national laws designed to accuse criminals to the test. (Choi & Parti, 2022).

According to Singh et al. (2023), the proliferation of IoT devices and the nationwide installation of 5G will increase the surface area at risk of cyberattacks. It seems likely that ransomware, sophisticated financial crimes, and data breaches aimed at businesses will keep on increasing. An increasing number of additional issues are being reported in Bangladesh every day, involving ransomware, spam, identity theft, cyberbullying, and web-based attacks. These problems remain because people continue to be careless in following the aforementioned rules and methods, despite significant efforts already made by the Bangladeshi government. Issues that remain unresolved will decline as individuals learn to be mindful of their digital footprint.

9. Conclusion

Bangladesh's rapidly evolving digital landscape presents both opportunities and significant risks. Although the incidence of major cybercrimes has been relatively low so far, the increasing dependence on digital technologies in sectors like finance heightens the risk of such crimes (Zakaria, 2023). Fusi et al. (2023) argue that the country's existing legislative and technological frameworks are inadequate to address the complex and ever-changing cyber threats emerging globally. This vulnerability is exacerbated by low public awareness and weak enforcement of current cyber laws. To address these challenges, Bangladesh must proactively enhance its cybersecurity infrastructure by strengthening international collaboration, investing in advanced cyber technologies, and increasing public awareness of cyber threats. Bangladesh needs to develop and implement comprehensive strategies to tackle future cyber threats. According to Zakaria (2023), this involves not only updating and enforcing cyber laws but also promoting ethical behavior and providing support to cybercrime victims. By adopting these measures, Bangladesh can better safeguard its digital future, mitigate the risks posed by cybercriminals, and ensure a secure and resilient online environment for all.

Acknowledgement:

The researchers extend their appreciation to Mohammad Rakibul Islam Bhuiyan, a faculty member of Begum Rokeya University in Rangpur, Bangladesh, for his valuable insights. Insufficient financial resources are available to carry out this research. No external funding has been received for conducting

this study. This study report is free from any conflicts of interest. All authors have contributed equally to every part of the study.

Copyright:

References

[1] Abthal Abdajabar, & Tarik Idbeaa. (2024). Cybercrime's threat to financial institutions during COVID-19. *AlQalam Journal of Medical and Applied Sciences*, 46-52. https://doi.org/10.54361/ajmas.2472207

[2] Achaal, B., Adda, M., Berger, M., Ibrahim, H., & Awde, A. (2024). Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. *Cybersecurity*, *7*(1). https://doi.org/10.1186/s42400-023-00200-w

[3] Akter, M. S., Bhuiyan, M. R. I., Poli, T. A., & Hossain, R. (2023). Web-based Banking Services on E-Customer Satisfaction in Private Banking Sectors: A Cross-Sectional Study in Developing Economy. Migration Letters, 20(S3), 894-911. https://doi.org/10.59670/ml.v20iS3.3976

[4] Akter, M. S., Bhuiyan, M. R. I., Tabassum, S., Alam, S. A., Milon, M. N. U., & Hoque, M. R. (2023). Factors Affecting Continuance Intention to Use E-wallet among University Students in Bangladesh. https://doi.org/10.14445/22315381/IJETT-V71I6P228

[5] Alexandrou, A. (2021). Laws, standards, and regulations affecting cybercrime. *Cybercrime and Information Technology*, 105-170. https://doi.org/10.4324/9780429318726-4

[6] Ali, A. (2019). Digital literacy and the spread of misinformation in Pakistan. *AEA Randomized Controlled Trials*. https://doi.org/10.1257/rct.4003-3.0

[7] Amin, A., Bhuiyan, M. R. I., Hossain, R., Molla, C., Poli, T. A., & Milon, M. N. U. (2024). The adoption of Industry 4.0 technologies by using the technology organizational environment framework: The mediating role to manufacturing performance in a developing country. *Business Strategy & Development*, *7*(2), e363. https://doi.org/10.1002/bsd2.363

[8] Anzelone, C., & Katz, L. (2024). Behavioral interventions to advance self sufficiency next generation (BIAS-NG), Wayne County head start attendance. *AEA Randomized Controlled Trials*. https://doi.org/10.1257/rct.13272-1.0

[9] Barnor, J. N., & Patterson, A. A. (2020). Cybercrime research. *Advances in Information Quality and Management*, 480-502. https://doi.org/10.4018/978-1-7998-2610-1.ch024

[10] Bhardwaj, A. (2023). Security challenges for cloud-based email infrastructure. *New Age Cyber Threat Mitigation for Cloud Computing Networks*, 133-151. https://doi.org/10.2174/9789815136111123010012

[11] Bhuiyan, M. R. I. (2023). The Challenges and Opportunities of Post-COVID Situation for Small and Medium Enterprises (SMEs) in Bangladesh. *PMIS Review*, *2*(1), 141-159. http://dx.doi.org/10.56567/pmis.v2i1.14

[12] Bhuiyan, M. R. I. (2024). Examining the digital transformation and digital entrepreneurship: A PRISMA based systematic review. Pakistan Journal of Life and Social Sciences, *22*(1), 1136-1150. http://dx.doi.org/10.57239/PJLSS-2024-22.1.0077

[13] Bhuiyan, M. R. I., Akter, M. S., & Islam, S. (2024). How does digital payment transform society as a cashless society? An empirical study in the developing economy. *Journal of Science and Technology Policy Management*. Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JSTPM-10-2023-0170

[14] Bhuiyan, M. R. I., Faraji, M. R., Rashid, M., Bhuyan, M. K., Hossain, R., & Ghose, P. (2024). Digital Transformation in SMEs Emerging Technological Tools and Technologies for Enhancing the SME's Strategies and Outcomes. *Journal of Ecohumanism*, *3*(4), 211-224. https://doi.org/10.62754/joe.v3i4.3594

[15] Bhuiyan, M. R. I., Hossain, R., Rashid, M., Islam, M. M., Mani, L., & Milon, M. N. U. (2024). Gravitating the components, technologies, challenges, and government transforming strategies for a Smart Bangladesh: A PRISMA-based review. *Journal of Governance and Regulation*, *13*(3), 177–188. https://doi.org/10.22495/jgrv13i3art15

[16] Bhuiyan, M. R. I., Uddin, K. S., & Milon, M. N. U. (2023). Prospective Areas of Digital Economy in the Context of ICT Usages: An Empirical Study in Bangladesh. *FinTech*, *2*(3), 641-656. https://doi.org/10.3390/fintech2030035

[17] Bhuiyan, M. R. I., Ullah, M. W., Ahmed, S., Bhuyan, M. K., & Sultana, T. (2024). Information Security for An Information Society for Accessing Secured Information: A PRISMA Based Systematic Review. *International Journal of Religion*, *5*(11), 932-946. https://doi.org/10.61707/frfnr583

[18] Bhuiyan, M. R., & Akter, M. (2024). Assessing the Potential Usages of Blockchain to Transform Smart Bangladesh: A PRISMA Based Systematic Review. *Journal of Information Systems and Informatics*, *6*(1), 245-269. https://doi.org/10.51519/journalisi.v6i1.659

[19] Bhukta, A. (2020). How fit are the existing intellectual property rights laws in protecting traditional knowledge? *Legal Protection for Knowledge*, 125-138. https://doi.org/10.1108/978-1-80043-063-120200007

[20] Buettner, R., Blattner, M., & Reinhardt, W. (2020). Internet gaming more than 3 hours a day is indicative and more than 5 hours is diagnostic: Proposal of playing time Cutoffs for WHO-11 and DSM-5 internet gaming disorder based

on a large steam platform dataset. *2020 IEEE Sixth International Conference on Big Data Computing Service and Applications (BigDataService)*. https://doi.org/10.1109/bigdataservice49289.2020.00037

[21] Chamakiotis, P., McKenna, B., Bednar, K., & Chughtai, H. (2024). From technology and virtuality to "Our digital lives". *IFIP Advances in Information and Communication Technology*, 59-88. https://doi.org/10.1007/978-3-031-50758-8_5

[22] Chandra, R., & Singh, S. (2024). Digital inequalities: Its impact on quality of life among the young generation. *Contemporary Social Sciences*, *33*(1), 59-65. https://doi.org/10.62047/css.2024.03.31.59

[23] Choi, J., Dulisse, B., & Han, S. (2023). Assessing the overlap between cyberstalking victimization and face-to-face sexual victimization among South Korean middle and high school students. *The Link between Specific Forms of Online and Offline Victimization*, 40-58. https://doi.org/10.4324/9781003429678-4

[24] Choi, S., & Parti, K. (2022). Understanding the challenges of cryptography-related cybercrime and its investigation. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(2), 1-3. https://doi.org/10.52306/2578-3289.1134

[25] Ciuchi, C. (2022). Developing a comprehensive model for digital lifelong learning using cyber resilience framework. *Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3)*. https://doi.org/10.19107/cybercon.2022.14

[26] Collier, A. B. (2020). Emayili: Send email messages. *CRAN: Contributed Packages*. https://doi.org/10.32614/cran.package.emayili

[27] Corbet, S., Cumming, D. J., Hou, Y. (., Hu, Y., & Oxley, L. (2022). Have crisis-induced banking supports influenced European bank performance, resilience and price discovery? *Journal of International Financial Markets, Institutions and Money*, *78*, 101566. https://doi.org/10.1016/j.intfin.2022.101566

[28] Dewi, Y., Suharman, H., Sofia Koeswayo, P., & Dewi Tanzil, N. (2023). Factors influencing the effectiveness of credit card fraud prevention in Indonesian issuing banks. *Banks and Bank Systems*, *18*(4), 44-60. https://doi.org/10.21511/bbs.18(4).2023.05

[29] Du Toit, P. G. (2023). The search warrant provisions of the cybercrimes act and their relationship with the Criminal Procedure Act. *Obiter*, *43*(4). https://doi.org/10.17159/obiter.v43i4.13191

[30] Duckert, M., & Barkhuus, L. (2022). Protecting personal health data through privacy awareness. *Proceedings of the ACM on Human-Computer Interaction*, *6*(GROUP), 1-22. https://doi.org/10.1145/3492830

[31] Dumberry, P. (2018). Requiem for Crimea: Why tribunals should have declined jurisdiction over the claims of Ukrainian investors against Russian under the Ukraine–Russia BIT. *Journal of International Dispute Settlement*, *9*(3), 506-533. https://doi.org/10.1093/jnlids/idy022

[32] Ebegba, R., & Onwude, J. (2022). Emerging technologies. *Biosafety and Bioethics in Biotechnology*, 43-49. https://doi.org/10.1201/9781003179177-4

[33] Elegbe, I. (2024). Cybercrime legislation: A comparative analysis of legal frameworks, policy responses and recommendations. *International Journal of Education and Social Science Research*, *07*(02), 199-207. https://doi.org/10.37500/ijessr.2024.7211

[34] Evans, D. S. (2023). Some economic aspects of artificial intelligence technologies and their expected social value. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4553857

[35] Fusi, F., Jung, H., & Welch, E. (2023). Technological vulnerability and knowledge of cyber-incidents: Threats to innovativeness in local governments? *Public Management Review*, 1-27. https://doi.org/10.1080/14719037.2023.2250362

[36] Gadallah, W. G., Ibrahim, H. M., & Omar, N. M. (2024). A deep learning technique to detect distributed denial of service attacks in software-defined networks. *Computers & Security*, *137*, 103588. https://doi.org/10.1016/j.cose.2023.103588

[37] Gökdemir, B. (2021). Regulation of fixed telecommunication services. *The Regulation of Turkish Network Industries*, 365-382. https://doi.org/10.1007/978-3-030-81720-6_18

[38] Heffernan, L., & O'Connor, E. (2020). Threats to security and risks to rights: 'Belief evidence' under the offences against the state act. *The Offences Against the State Act 1939 at 80*. https://doi.org/10.5040/9781509932023.ch-006

[39] Her, P., Saeed, S., Tram, K. H., & Bhatnagar, S. R. (2021). Can tracking mobility be used as a public health tool against COVID-19 following the expiration of stay-at-home mandates? https://doi.org/10.1101/2021.08.27.21262629

[40] Hillebrand, K., & Hornuf, L. (2020). The social dilemma of big data. *AEA Randomized Controlled Trials*. https://doi.org/10.1257/rct.6241

[41] Hossain, R., Al- Amin, A.-A., Mani, L., Islam, M. M., Poli, T. A., & Milon, M. N. U. (2024). Exploring the Effectiveness of Social Media on Tourism Destination Marketing: An Empirical Study in a Developing Country. *WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS*, *21*, 1392–1408. https://doi.org/10.37394/23207.2024.21.114

[42] Ilushin, D. (2024). Transfer of responsible data using open communication channels. *Intelligent transport systems*. https://doi.org/10.30932/9785002446094-2024-584-587

[43] Islam, M. A., & Bhuiyan, M. R. I. (2022). Digital Transformation and Society. Available at SSRN: https://ssrn.com/abstract=4604376 or http://dx.doi.org/10.2139/ssrn.4604376

[44] Islam, Z., Bhuiyan, M. R. I., Poli, T. A., Hossain, R., & Mani, L. (2024). Gravitating towards Internet of Things: Prospective Applications, Challenges, and Solutions of Using IoT. *International Journal of Religion*, *5*(2), 436-451. https://doi.org/10.61707/awg31130

[45] Jadhav, A. (2024). Data protection in India: Legal frameworks and emerging trends. *Personal Data Protection In Digital Age: Issues And Challenges*. https://doi.org/10.59646/dataprotectionc19/125

[46] Jones, A., Horsburgh, J., & Flint, C. (2022). Hydroinformatics and water data science instructor interviews and surveys. *HydroShare Resources*. https://doi.org/10.4211/hs.15b1a61f47724a6e8deb100789353df2

[47] Joshi, R., & Rehman, S. (2023). Raising awareness of social engineering among adolescents. *Cybersecurity for Decision Makers*, 99-109. https://doi.org/10.1201/9781003319887-7

[48] Kabir, M. R., Hossain, R., Rahman, M. M., Sawon, M. M. H., & Mani, L. (2024). Impact of E-Marketing on Book Purchase Tendencies: An Empirical Study on University Undergraduate Students. *Journal of Ecohumanism*, *3*(3), 612-631. https://doi.org/10.62754/joe.v3i3.3388

[49] Kadeni, K. (2023). Upaya meningkatkan kompetensi guru dalam menggunakan media pembelajaran online melalui kegiatan webinar Di smp negeri 2 selat kabupaten kapuas tahun pelajaran 2020/2021. *Anterior Jurnal*, *22*(3), 1-9. https://doi.org/10.33084/anterior.v22i3.5689

[50] Kaium, M. A., Nuery, N., & Ghosh, P. (2019). THE IMPACT OF SCRM ON RETENTION OF CUSTOMERS: A CASE STUDY ON SOCIAL ISLAMIC BANK LIMITED. *BARISHAL UNIVERSITY JOURNAL (PART-3) A JOURNAL OF BUSINESS STUDIES*, *1719398694*, 61.

[51] Kalėda, S. L. (2023). New European Union's regulatory framework of the digital space: The digital markets act and the digital services act. *Teisė*, *127*, 25-42. https://doi.org/10.15388/teise.2023.127.2

[52] Kikerpill, K. (2023). The crime-as-communication approach: Challenging the idea of online routine activities by taking communication seriously. *Journal of Economic Criminology*, *2*, 100035. https://doi.org/10.1016/j.jeconc.2023.100035

[53] Kim, S., & Yong Jin, D. (2024). How Korea's digital platforms have been evolved? *Korea's Platform Empire*, 21-45. https://doi.org/10.4324/9781003441694-2

[54] Kirtz, J. L. (2018). Beyond the Blackbox: Repurposing ROM hacking for feminist hacking/Making practices. *Ada: A Journal of Gender, New Media, and Technology*, (13). https://doi.org/10.5399/uo/ada.2018.13.3

[55] Kluener, L., Chan, K., & Antoniades, C. (2024). Using artificial intelligence to study atherosclerosis from computed tomography imaging: A state-of-the-art review of the current literature. *Atherosclerosis*, 117580. https://doi.org/10.1016/j.atherosclerosis.2024.117580

[56] Koen, C. (2020). Significance levels of common frequencies extracted from multiple data sets. *Monthly Notices of the Royal Astronomical Society*, *493*(1), 48-54. https://doi.org/10.1093/mnras/staa190

[57] Kumar, K. S. (2017). Article 133: Appellate jurisdiction of Supreme Court in appeals from high courts in regard to civil matters. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3078848

[58] Kundu, A., & Plambeck, E. (2024). Development and assessment of business model innovation to increase adoption of longer lasting electric three Wheeler batteries in Bangladesh. *AEA Randomized Controlled Trials*. https://doi.org/10.1257/rct.14061-1.0

[59] Lamé, D. (2019). Trust towards immigrants. *AEA Randomized Controlled Trials*. https://doi.org/10.1257/rct.5193-1.2000000000000002

[60] Lanza, C., Lahmadi, A., & Osmond, F. (2024). An empirical study of ransomware vulnerabilities descriptions. *Proceedings of the 10th International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0012378700003648

[61] Levin, A. (2023). How the battle against cybercrime strengthens sustainable finance. *Sustainable Finance*, 329-352. https://doi.org/10.1007/978-3-031-28752-7_17

[62] Liu, Y. (2023). The lack of contemporary death education in China and its impact on public awareness. *Lecture Notes in Education Psychology and Public Media*, *8*(1), 104-108. https://doi.org/10.54254/2753-7048/8/20230055

[63] Lizunov, P., Biloshchytskyi, A., Kuchansky, A., & Andrashko, Y. (2021). Combined methods for identifying incomplete duplicates in scientific publications. *Management of Development of Complex Systems*, (48), 85-94. https://doi.org/10.32347/2412-9933.2021.48.85-94

[64] Lucila Jr., N., & Ching, M. R. (2024). Digital inclusion in agriculture: Profiling the factors influencing social commerce adoption among farm cooperatives. https://doi.org/10.2139/ssrn.4867052

[65] Mani, L. (2024). Gravitating towards the Digital Economy: Opportunities and Challenges for Transforming Smart Bangladesh. *Pakistan Journal of Life and Social Sciences*. 22(1), 3324-3334, https://doi.org/10.57239/PJLSS-2024-22.1.00241

[66] Meah, M. R., & Hossain, R. (2023). Ownership structure and auditor choice in emerging economy: An empirical study. *Indonesian Journal of Business, Technology and Sustainability*, *1*(1), 12-22.

[67] Meng, J., & Li, W. (2023). How to combat cyber scams? A randomized control trial on a major online payment platform in China. *AEA Randomized Controlled Trials*. https://doi.org/10.1257/rct.11899-1.0

[68] Mittal, C. (2024). An empirical study on cybersecurity awareness, cybersecurity concern, and vulnerability to cyber-attacks. *International Journal of Scientific Research and Management (IJSRM)*, *12*(04), 1144-1158. https://doi.org/10.18535/ijsrm/v12i04.ec05

[69] Molla, C., Mani, L., Bhuiyan, M. R. I., & Hossain, R. (2023). Examining the Potential Usages, Features, and Challenges of Using ChatGPT Technology: A PRISMA-Based Systematic Review. *Migration Letters*, *20*(S9), 927-945. https://doi.org/10.59670/ml.v20iS9.4918

[70] Momtaz, M. S. (2024). 'Navigating cyber security challenges and legal frameworks in Bangladesh: An in-depth exploration'. *International Journal of Research and Innovation in Social Science*, *VIII*(I), 727-751. https://doi.org/10.47772/ijriss.2024.801056

[71] Petersen, K., Copson, S., & Anagnostou, A. (2023). Evaluating the ethical and societal impacts of modelling pandemic crises: Experiences from a workshop. *Proceedings of SW21 The OR Society Simulation Workshop*, 184-193. https://doi.org/10.36819/sw23.022

[72] Poli, T. A., Sawon, M. M. H., Mia, M. N., Ali, W., Rahman, M., Hossain, R., & Mani, L. (2024). Tourism And Climate Change: Mitigation And Adaptation Strategies In A Hospitality Industry In Bangladesh. *Educational Administration: Theory and Practice*, *30*(5), 7316-7330. https://doi.org/10.53555/kuey.v30i5.3798

[73] Poli, T. A. (2024). Mediating Role of Entrepreneurship Capability in Sustainable Performance and Women Entrepreneurship: An Evidence from a Developing Country. *Journal of Ecohumanism*, *3*(3), 2006-2019. https://doi.org/10.62754/joe.v3i3.3553

[74] Prasetyo, S. E., Haeruddin, H., & Ariesryo, K. (2024). Website security system from denial of service attacks, SQL injection, cross site scripting using web application firewall. *Antivirus : Jurnal Ilmiah Teknik Informatika*, *18*(1), 27-36. https://doi.org/10.35457/antivirus.v18i1.3339

[75] Priom, M. A. I., Mudra, S. L., Ghose, P., Islam, K. R., & Hasan, M. N. (2024). Blockchain Applications in Accounting and Auditing: Research Trends and Future Research Implications. *International Journal of Economics, Business and Management Research*, 8(7), 225-247.

[76] Radanliev, P. (2024). undefined. *Journal of Cyber Security Technology*, 1-51. https://doi.org/10.1080/23742917.2024.2312671

[77] Rahman, Md. M., Islam, Md. M., Khatun, M., Uddin, S., Faraji, M. R., & Hasan, Md. H. (2024). Gravitating towards Information Society for Information Security in Information Systems: A Systematic PRISMA Based Review. *Pakistan Journal of Life and Social Sciences (PJLSS)*, *22*(1). https://doi.org/10.57239/PJLSS-2024-22.1.0089

[78] Ramírez, V. A., & Prada, J. D. (2024). Study and analysis of Cyberterrorist attacks from hybrid computer systems under the quantum spectrum of software development and data processing; Colombia national police. *INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH*, *12*(01). https://doi.org/10.47191/ijmcr/v12i1.06

[79] Rickards, P. (2023). Measuring the effect of the media on the public's understanding of Central Bank information. *AEA Randomized Controlled Trials*. https://doi.org/10.1257/rct.10748-1.3

[80] Saha, S., Sen, K. K., & Bishwas, P. C. (2024). Nexus between Economic Policy Uncertainty and Bank Liquidity Creation: Moderating Role of Bank Regulations and Credit Risk. Finance & Economics Review, 6(1), 45-60. https://doi.org/10.38157/fer.v6i1.621

[81] Samarkina, Y. E. (2023). Procedural role of the prosecutor in court of original jurisdiction and Court of Appeal in criminal cases. *Теория и практика общественного развития*, (2), 149-152. https://doi.org/10.24158/tipor.2023.2.21

[82] Saul, B., & Heath, K. (2021). Cyber terrorism and use of the internet for terrorist purposes. *Research Handbook on International Law and Cyberspace*. https://doi.org/10.4337/9781789904253.00020

[83] Saxena, M. (2023). Impact of cybercrime on E-governance. Is cybercrime affecting the confidentiality of government data? *International Journal of Science and Research (IJSR)*, *12*(11), 911-915. https://doi.org/10.21275/sr231111140516

[84] Sharma, V. (2022). Cybercrimes and digital forensics in Internet of things. *Internet of Things and Cyber Physical Systems*, 209-229. https://doi.org/10.1201/9781003283003-10

[85] Sleem, A. (2022). A comprehensive study of cybersecurity threats and countermeasures: Strategies for mitigating risks in the digital age. *Journal of Cybersecurity and Information Management*, *10*(2), 35-46. https://doi.org/10.54216/jcim.100204

[86] Spence, K., & Clapton, G. (2018). Gender balance in the childcare workforce: Why having more men in childcare is important. *Oxford Scholarship Online*. https://doi.org/10.1093/oso/9780198747109.003.0010

[87] Strader, S. M., Gensini, V. A., Ashley, W. S., & Wagner, A. N. (2024). Changes in tornado risk and societal vulnerability leading to greater tornado impact potential. *npj Natural Hazards*, *1*(1). https://doi.org/10.1038/s44304-024-00019-6

[88] Tadi, V. (2023). Trust and behavior in the digital age: Adapting regulatory frameworks to enhance adoption and efficacy of secure payment technologies. *International Journal of Science and Research (IJSR)*, *12*(5), 2683-2691. https://doi.org/10.21275/sr24716122121

[89] Vaishy, S., & Gupta, H. (2021). Cybercriminals' motivations for targeting government organizations. *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. https://doi.org/10.1109/icrito51393.2021.9596104

[90] Venkatachary, S. K., Prasad, J., Alagappan, A., Andrews, L. J., Raj, R. A., & Duraisamy, S. (2024). Cybersecurity and cyber-terrorism challenges to energy-related infrastructures – Cybersecurity frameworks and economics –

Comprehensive review. *International Journal of Critical Infrastructure Protection*, *45*, 100677. https://doi.org/10.1016/j.ijcip.2024.100677

[91] Verma, K. (2021). IP-CHOCK reference detection and prevention of denial of service (Dos) attacks in vehicular ad-hoc network. *Research Anthology on Combating Denial-of-Service Attacks*, 579-601. https://doi.org/10.4018/978-1-7998-5348-0.ch030

[92] Verma, V., & Pawar, J. (2024). Assessment of students cybersecurity awareness and strategies to safeguard against cyber threats. *Journal of Advanced Zoology*, 82-89. https://doi.org/10.53555/jaz.v45is4.4156

[93] Vyas, D. (2023). Influencing factors for Indian customers' purchase intentions for online shopping. *International Journal of Indian Culture and Business Management*, *1*(1). https://doi.org/10.1504/ijicbm.2023.10061081

[94] Wang, Y., & Li, K. (2024). How do official software citation formats evolve over time? A longitudinal analysis of R programming language packages. *Scientometrics*, *129*(7), 3997-4019. https://doi.org/10.1007/s11192-024-05064-6

[95] Widodo, M., Weiner, A. M., Zubaedah, P. A., Prayitno, A. H., & Andriani, F. (2024). International legal dynamics in combating cybercrime: Challenges and opportunities for developing countries. *Global International Journal of Innovative Research*, *2*(1). https://doi.org/10.59613/global.v2i1.49

[96] Zahra, R. A., Amiruloh, M., & Rafianti, L. (2023). Legal protection of bank financial institution brand against Username squatting through Twitter accounts based on the trademark law and the electronic information and transaction law. *COMSERVA : Jurnal Penelitian dan Pengabdian Masyarakat*, *3*(06), 2139-2148. https://doi.org/10.59141/comserva.v3i06.1026

[97] Zakaria, P. (2023). Financial inclusion to digital finance risks: A commentary on financial crimes, money laundering, and fraud. *Financial Innovation and Technology*, 123-130. https://doi.org/10.1007/978-3-031-17998-3_9

[98] Zhang, J. (2024). Research on perceived usefulness & Perceived ease of use and online shopping intention. *Journal of New Media and Economics*, *1*(1), 22-30. https://doi.org/10.62517/jnme.202410104

[99] Zhang, X., Liu, Y., Qin, Z., Ye, Z., & Meng, F. (2023). Understanding the role of social media usage and health self-efficacy in the processing of COVID-19 rumors: A SOR perspective. *Data and Information Management*, *7*(2), 100043. https://doi.org/10.1016/j.dim.2023.100043

[100] Zhuk, A. (2024). Crypto-anarchy: A paradigm shift for society and the legal system. *Journal of Computer Virology and Hacking Techniques*. https://doi.org/10.1007/s11416-024-00525-1