CYBER READINESS OF THE LAW ENFORCEMENT AGENCIES TO COMBAT CYBER TERRORISM IN BANGLADESH

Arman Hossain [1], Kazi Murad Hossain [2] & Shilajit Kumar Roy[3]

ABSTRACT

The internet has revolutionized human interaction, providing an essential platform for communication, information exchange, and economic development. As societies become increasingly digital, the internet has also emerged as a double-edged sword, introducing a host of cyber threats that jeopardize security and privacy. For Bangladesh, a developing country striving for progress in the digital landscape, these threats present a significant challenge. Law enforcement agencies in Bangladesh play a crucial role in addressing the growing threats. This study aims to assess the preparedness of Bangladeshi law enforcement in countering cyber-terrorism and examines the challenges they face in securing cyberspace. Through a mixed-methods approach, combining interviews with Assistant Superintendents of Police (ASPs) and Officers-in-Charge (OCs) and questionnaires distributed among Sub-Inspectors (SIs) and Assistant Sub-Inspectors (ASIs), the study provides insights into current limitations and preparedness levels. Recent incidents reveal critical security gaps, underscoring the need for advanced training, updated legal frameworks, and enhanced resources. The findings emphasize the importance of strategic reforms to empower law enforcement agencies and reduce vulnerabilities. Recommendations for strengthening cyber security protocols are proposed to build a resilient framework against cyber-terrorism in Bangladesh.

Keywords: Cyberterrorism, Law Enforcement Agency, Bangladesh

[1] Lecturer, Department of Law, Bangladesh University, Dhaka - 1207, Bangladesh
[2] Assistant Professor, Law Discipline, Khulna University, Khulna - 9208, Bangladesh
[3] LL.B. (Hons.), LL.M. (Pursuing), Khulna University, Khulna - 9208, Bangladesh

1. Introduction

Cyber-terrorism, which involves using computer networks to disrupt essential national services like energy, transportation, and government operations, poses a significant and growing threat to Bangladesh. As the country progresses towards its 'Digital Bangladesh' vision under Vision 2021, it faces increasing vulnerabilities in cyberspace due to the surge in internet use and technological adoption. Recent incidents, such as the Bangladesh Bank heist and attacks on financial and government institutions, highlight these cyber security challenges. While law enforcement agencies have long recognized the risks associated with cyber threats, the sophistication and frequency of cyber-attacks have accelerated. This evolving threat landscape requires substantial advancements in technology, legal frameworks, and user awareness to safeguard against future attacks. As cyber-terrorism becomes an international concern, Bangladesh must strengthen its law enforcement capabilities to minimize risks. Based on this context, this paper seeks to examine the current preparedness of these agencies and propose necessary measures for adapting to this growing challenge.

1.1 Objectives of the study

This study aims to address the following objectives:

i. To examine the current state of cyber-terrorism in Bangladesh.

ii. To assess the preparedness and capabilities of law enforcement agencies in addressing this growing threat.

iii. To identify the significant challenges facing Bangladeshi law enforcement in combating cyber-terrorism and recommend essential measures for strengthening their response.

1.2 Methodology of the study

This study adopts a mixed-methods approach. Primarily, a qualitative research approach has been applied to evaluate current policies and analyze challenges in combating cyber terrorism. Additionally, a quantitative approach categorizes, analyzes, and tabulates primary data according to the study's objectives and variables. Data are drawn from both primary and secondary sources to capture trends and the evolving cyber threat landscape in Bangladesh.

Primary data include laws relating to cyberterrorism, interviews and questionnaires with law enforcement personnel, including police officers directly involved in handling cyberterrorism. Secondary data sources include newspaper articles, blogs, websites, etc.

1.3 Sample and Data Collection Methods

The study includes a diverse group of law enforcement personnel to obtain a well-rounded view of cyber terrorism response across different ranks. Data will be collected from two Assistant Superintendents of Police (ASPs) and three Officers-in-Charge (OCs) through interviews to gain insights into strategic and operational challenges in cyber security. Additionally, questionnaires will be administered to 14 Sub-Inspectors (SIs) and six Assistant Sub-Inspectors (ASIs), enabling structured data collection from those on the front lines.

2. Conceptual Discussion

2.1 What is cyber-terrorism?

Cyber terrorism refers to intentional attacks on computer systems, data, programs, or other digital assets,[4] aimed at causing harm and violence against individuals, organizations, or subnational groups. The primary objective of cyberterrorism is to inflict damage and fear.[5] A subset of cyber terrorism is internet terrorism, where individuals and groups exploit the anonymity of the internet to threaten or target specific individuals, communities, religions, nationalities, or ideologies. Cyberterrorism can be categorized into three broad types based on the complexity and scale of the attacks. Simple cyberterrorism involves basic attacks, such as hacking into a single system, often with limited impact. Advanced cyberterrorism represents a more sophisticated level of threat, where multiple systems and networks are compromised, increasing the potential for disruption. Finally, Complex cyberterrorism consists of highly coordinated attacks that utilize advanced techniques and strategies, resulting in widespread disruption and significant consequences. Each category reflects a different level of threat, requiring law enforcement agencies to adapt their responses accordingly.

[4] 'Definition of CYBERTERRORISM' (*Merriam-Webster*) <https://www.merriam-webster.com/dictionary/cyberterrorism> accessed 2 November 2024.
[5] 'Cyber Terrorism' (*Wigan Council*) <https://www.wigan.gov.uk/Resident/Crime-Emergencies/Counter-terrorism/Cyber-terrorism.aspx> accessed 2 November 2024.

2.2 Methods used for cyber-terrorism

Cyber terrorist organizations aim to create widespread chaos, disrupt critical infrastructure, support political activism, and inflict bodily harm or even death. To achieve these goals, they employ a variety of attack tactics.[6] One such tactic is Advanced Persistent Threat (APT) assaults, which utilize sophisticated and stealthy methods to gain prolonged access to networks, allowing attackers to steal sensitive data without detection. Additionally, computer viruses, worms, and malware target information technology control systems, disrupting essential services in utilities, transportation, power grids, and military operations. Another common method is hacking, which involves gaining unauthorized access to sensitive information held by institutions, governments, and businesses. Ransomware is a particularly nefarious type of malware that encrypts data or information systems, demanding a ransom for decryption. Finally, phishing attacks aim to gather personal information through deceptive emails, using that information to infiltrate systems or steal the victim's identity. Together, these tactics illustrate the diverse and evolving landscape of cyber terrorism threats.

2.3 Cyber-terrorism in Bangladesh

Since independence, Bangladesh has faced various terrorist incidents, but these activities were not initially conducted in cyberspace. However, as the country has advanced technologically, it has witnessed several cyber threats. The threat of cyber terrorism to Bangladesh's technical infrastructure is both real and immediate. Hackers are increasingly targeting computers and servers, with attacks becoming more frequent and sophisticated. As Bangladesh's critical infrastructure becomes more reliant on information technology, it faces greater exposure to both foreign and domestic attacks.[7] There has been a marked rise in cyber incidents, including hacking, data breaches, and ransomware attacks targeting government agencies, financial institutions, and critical infrastructure.

2.4 Recent incidents of cyber-terrorism in Bangladesh

In 2021, Bangladesh experienced a significant cyberattack affecting at least 147 public and

[6] Rahul Awati, Robert Sheldon and Katie Terrell Hanna, 'What Is Cyberterrorism?' (*Tech Target*) <https://www.techtarget.com/searchsecurity/definition/cyberterrorism> accessed 2 November 2024.
[7] Ashiquddin Maruf, Md Rabiul Islam and Bulbul Ahamed, 'Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies' (2014) 1 Northern University Journal of Law.

private organizations, including major entities like Bangladesh Bank and several financial institutions.[8] The Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT) reported vulnerabilities in over 200 Microsoft Exchange Servers (MES) used in the country, identifying the hacker group Hafnium as a key threat actor responsible for the attack. The agency emphasized the need for organizations to assess their systems for potential exploitation and recommended immediate patching and implementation of security measures. This incident underscores the vulnerabilities within Bangladesh's cyber landscape and highlights the importance of robust cybersecurity protocols across all sectors.

In February 2016, Bangladesh Bank (BB) fell victim to a sophisticated cyber heist that targeted its reserves at the New York Federal Reserve, resulting in the theft of approximately $951 million.[9] The hackers exploited vulnerabilities in the SWIFT messaging network to execute unauthorized transactions, with $81 million eventually funneled to accounts in the Philippines. The operation was meticulously planned, allowing the attackers to deploy custom malware that compromised the user credentials of BB officials, facilitating the unauthorized transfer of funds. The incident remains largely unresolved, raising serious concerns about the country's cyber security measures. A probe committee later found that lapses in security protocols, including the establishment of a direct connection to the SWIFT system, contributed to the breach, underscoring the need for improved vigilance and enhanced cybersecurity strategies.

Numerous phishing sites and campaigns have been identified targeting various sectors in Bangladesh, with the national COVID-19 vaccination site being the most frequently attacked.[10] According to the Bangladesh Cyber Threat Landscape 2022, mail service domains associated with all three branches of the Bangladesh Armed Forces, as well as the Rapid Action Battalion, were also targeted in these phishing campaigns.

[8] 'Cyber Attacks Hit over 200 Organizations Including Bangladesh Bank, BTRC' *Dhaka Tribune* (2 April 2021) <https://www.dhakatribune.com/bangladesh/242875/cyber-attacks-hit-over-200-organizations-including> accessed 2 November 2024.
[9] Rejaul Karim Byron and Md Fazlur Rahman, 'Bangladesh Bank Cyber Hacking: The Billion-Dollar Hit Job' *The Daily Star* (4 February 2020) <https://www.thedailystar.net/business/banking/bangladesh-bank-cyber-hacking-billion-dollar-hit-job-1863310> accessed 2 November 2024.
[10] 'Bangladesh Cyber Threat Landscape 2022' (BGD e-GOV CIRT) <https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/publications/effc311d_5097_46ba_afa4_5f44b60a93e6/Bangladesh%20Cyber%20Threat%20Landscape%202022.pdf>.

2.5 Legal measures to tackle cyber-terrorism in Bangladesh

The Cyber Security Act, 2023

Passed in 2023, this law protects against cyber terrorism, unlawful access to digital systems, and the spread of misinformation. It also regulates social media and digital platforms and imposes penalties for identity theft, digital fraud, and infringement of personal privacy. It establishes a dedicated Cyber Security Council and a Computer Security Incident Response Team (CSIRT) to coordinate responses to cyber incidents and facilitate collaboration among government, private sector, and civil society. The Act mandates the protection of critical information infrastructure (CII) across key sectors like banking and telecommunications, reducing vulnerabilities to potential attacks. It also requires organizations to report cyber incidents promptly, enabling quicker responses to threats.

The Anti-Terrorism Act, 2009

While primarily focused on general terrorism, the Act includes provisions for acts that disrupt public order and threaten national security, encompassing cyber-related offenses. The 2013 amendment stipulated that any discussions or conversations conducted by individuals or entities involved in terrorism on platforms such as Facebook, Skype, Twitter, or any other internet site, as well as any still images or videos related to their offenses, could be submitted as evidence to the court by law enforcement agencies for investigative purposes.

The Information and Communication Technology (ICT) Act, 2006

This law provides a framework for addressing cybercrimes, including fraud, data theft, and unauthorized access to computer systems. It also covers electronic transactions, ensuring the integrity and security of digital communications.

National Cyber Security Strategy 2021-2025

Although not a law *per se*, this strategy outlines the government's approach to enhancing cyber security and combating cyber threats, including terrorism. It aims to improve the resilience of critical infrastructure against cyberattacks.

3. Present status of law enforcement agencies dealing with cyber terrorism in Bangladesh

Various units within Bangladesh's law enforcement agencies are currently dedicated to countering cyber terrorism. While some units may not engage directly in combatting cyber terrorism, they provide crucial guidelines on effective countermeasures. Following are the departments that are directly involved in combatting cyber terrorism in Bangladesh, which include:

a. Special Branch (SB)

b. Detective Branch (DB)

c. Dhaka Metropolitan Police (DMP)

d. Anti-Terrorism Unit (ATU)

e. Counter Terrorism and Transnational Crime Unit (CTTC)

f. Rapid Action Battalion (RAB)

g. Cyber Security and Crime Division

h. Telecommunication and Information Management

i. Police Bureau of Investigation (PBI)

These units work directly to counter cyber-terrorism across Bangladesh. Additionally, certain sub-units actively participate 24/7, providing round-the-clock monitoring and support in cyber intelligence and counter-terrorism efforts. They are as follows:

Cyber Crime Investigation Division

Commonly known as the Cyber Crime Unit, this branch of Bangladesh Police operates under the Counter Terrorism and Transnational Crime (CTTC) division of the Dhaka Metropolitan Police. Its primary mission is to patrol, prevent, detect, and investigate cyber terrorism and cybercrimes within the metropolitan area. To effectively combat cyber threats, this division is

organized into four specialized monitoring teams:

i. Internet Referral

ii. Cyber Terrorism Investigation

iii. Digital Forensics

iv. E-Fraud Investigation

Cyber Police Center (CPC)

The Cyber Police Center (CPC) is a recent addition to the Criminal Investigation Department's (CID) long-standing tradition of training excellence. Established under the 'Enhancing the Cyber Investigation Capability of Bangladesh Police' project, funded by the Korean International Cooperation Agency (KOICA) and designed by Korean cyber experts, CPC aims to combat cybercrime in Bangladesh.[11] Inaugurated on January 23, 2017, CPC works towards a vision of a safe and secure digital Bangladesh by developing skilled personnel to protect cyberspace for all citizens.

With modern training facilities and qualified faculty, CPC has become a flagship center alongside the Detective Training School (DTS) and Forensic Training Institute (FTI). The CPC is dedicated to specialized training exclusively in cybercrime, cybersecurity, social media monitoring, and digital forensics.

Cyber Threat Intelligence Unit

The Cyber Threat Intelligence Unit of BGD e-GOV CIRT is dedicated to gathering and analyzing information on cyber threats and threat actors to help prevent harmful events within Bangladesh's cyberspace. This unit collects data through open-source intelligence, social media intelligence, and deep and dark web insights. Collaborating with several renowned threat intelligence services, the unit regularly provides comprehensive reports to Critical Information Infrastructure (CII) entities, financial institutions, and government agencies, enhancing

[11] 'Cyber Police Center' (*Criminal Investigation Department | Bangladesh Police*) <https://www.cid.gov.bd/public> accessed 2 November 2024.

national cybersecurity resilience.

Anti-Terrorism Unit (ATU)

The Anti-Terrorism Unit (ATU) conducts operations, investigations, and inquiries into individuals or entities involved in extremism, terrorism, terrorist activities, and terrorist financing through cyberspace. Within the ATU, two specialized teams, Cybercrime Monitoring and Cyber Forensics, closely monitor cyberspace to prevent cyber-terrorism.[12]

Police Cyber Support for Women (PCSW)

Police Cyber Support for Women (PCSW), an all-women initiative from the Bangladesh Police Headquarters, is dedicated to assisting women affected by cybercrimes.[13] Under the guidance of the Inspector General of Police, PCSW provides essential legal support and technological assistance to women victims while prioritizing the confidentiality of their information. Since its inception, PCSW has actively promoted cyber safety awareness, aiming to educate and protect women in the digital space. With a vision of creating a secure and tech-savvy environment, PCSW is committed to empowering women and fostering safer online interactions.

3.1 Strategies employed by law enforcement agencies

Addressing the threat of cyber-terrorism presents significant challenges, especially for developing countries. Effective strategies to combat cyber terrorism typically require a comprehensive approach, combining technical safeguards with robust legal frameworks. However, developing and implementing these tools takes time. The benefits of a strong anti-cyber terrorism strategy, including technical protections and network defenses, far exceed initial investments. The following discussion outlines the current readiness and initiatives of law enforcement agencies in Bangladesh to combat cyber terrorism.[14]

[12] 'Background' (*Anti Terrorism Unit, Bangladesh Police*) <https://atu.police.gov.bd/about-us/> accessed 2 November 2024.
[13] 'Police Cyber Support For Women' (*Bangladesh Police*) <https://www.police.gov.bd/en/police_cyber_support_for_women> accessed 2 November 2024.
[14] 'Towards Developing a Counter-Terrorism Policy for Bangladesh' (Bangladesh Enterprise Institute) <http://bei-bd.org/wp-content/uploads/2015/04/Towards-Developing-a-Counter-Terrorism-Policy-for-Bangladesh.pdf>.

3.1.1 Recent Instrumental Advancement

Dhaka Metropolitan Police (DMP) plans to purchase 15 types of digital equipment, referred to as "cyber arms," to enhance its ability to combat cyber terrorism. The planned purchases include tools like Cyber Guardian, real-time location-based social media monitoring systems, IP analyzers, hacking and intrusion software, advanced scanners, sketch-based image retrieval systems, and facial reconstruction tools, among other high-tech resources.

3.1.2 Operational Arrangements

Police and emergency services will initially respond to any incident, which may later be identified as a terrorist act. Once there is reasonable suspicion of terrorism, police will take control and notify the NCCT. In areas where Bangladesh Police has counter-terrorism units, Protective Service Officers will provide the first response until control is handed over to attending police.

3.1.3 Criminal Investigation

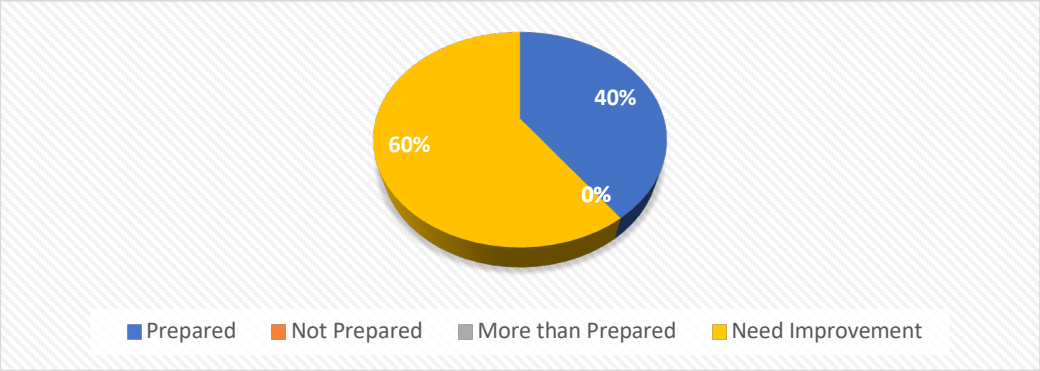
All law enforcement and intelligence agencies play a crucial role in detecting, preventing, and investigating terrorist activities, acting as first responders in the event of a terrorist incident. Terrorism is considered a crime under the Anti-Terrorism Act of 2009, and a specialized unit within the Bangladesh Police can be established to handle investigations related to terrorist incidents in cyberspace.

4. Findings

4.1 Questionnaire Survey

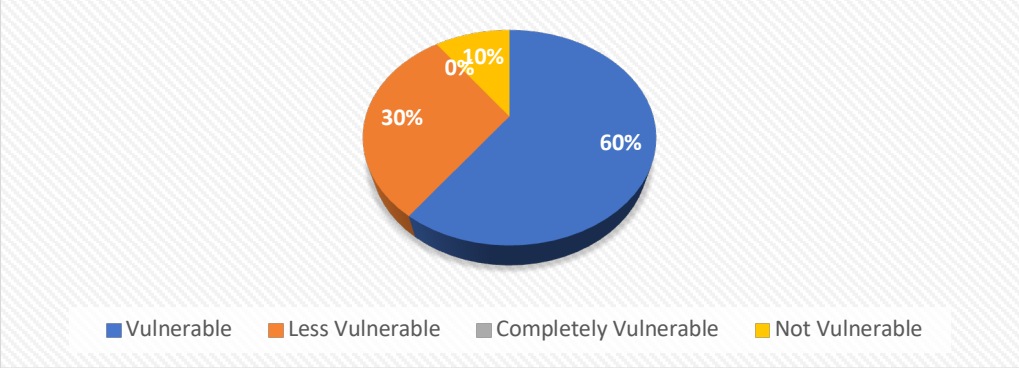
Since this study aims to identify the various challenges faced by law enforcement officials in carrying out their mandated responsibilities related to cyber terrorism in Bangladesh, insights were gathered from representatives of the Counter Terrorism Unit, Special Branch, Criminal Investigation Division, and Anti-Terrorism Unit. The officials were asked questions across nine different aspects to achieve the research objectives.

Is the law enforcement agency prepared to combat cyber terrorism in Bangladesh?



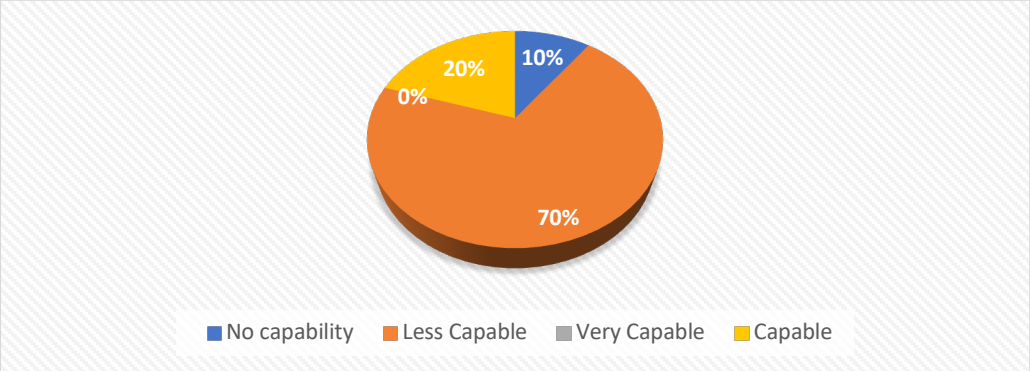
In response to this question, 60% of the total respondents indicated that law enforcement agencies are currently prepared to combat cyber terrorism, while 40% expressed the need for improvements within the agencies. No comments were provided regarding other options.

What is your evaluation of Bangladesh's vulnerability to cyber-attacks from terrorist groups?



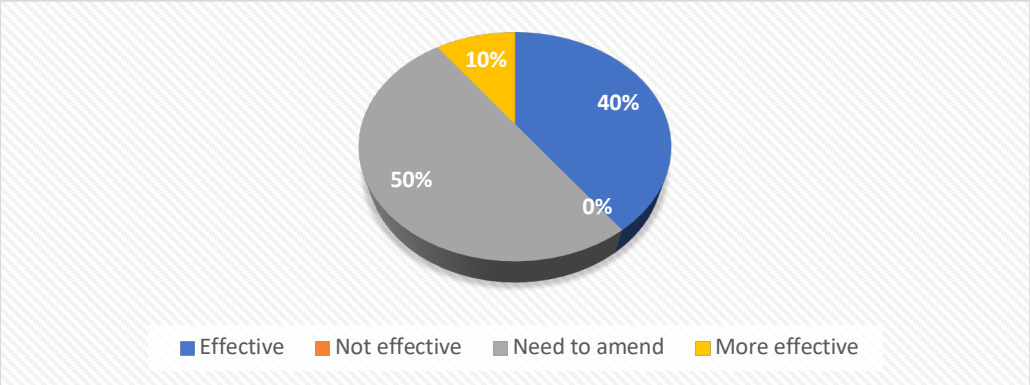
In response to this question, 60% of the total respondents stated that Bangladesh is vulnerable to cyber-attacks from terrorist groups, while 30% believed the country is less vulnerable. Additionally, 10% of respondents indicated that Bangladesh is not vulnerable at this time.

What is your evaluation of the capability of terrorist groups to execute cyber terrorism against Bangladesh?



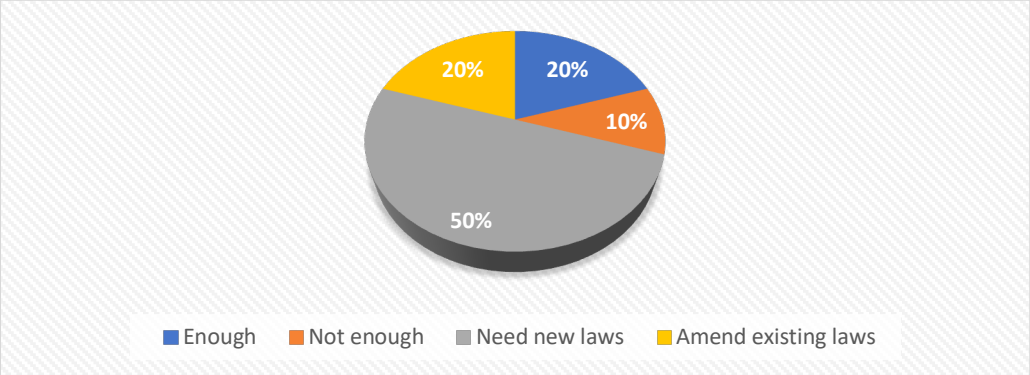
In response to this question, 70% of the total respondents indicated that terrorist groups are less capable of carrying out cyber-terrorism in Bangladesh. Meanwhile, 20% believed that these groups possess the capability, and 10% stated that they have no capability at all.

What is your evaluation of the effectiveness of the existing substantive and procedural laws in responding to cyber-terrorism in Bangladesh?



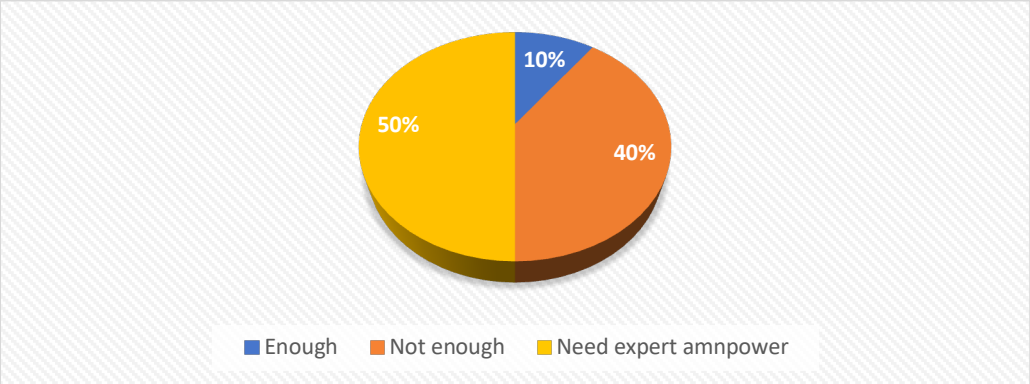
In response to this question, 50% of the total respondents stated that the existing substantive and procedural laws need to be amended to effectively address cyber-terrorism in Bangladesh. Meanwhile, 40% regarded the current laws as effective, and 10% felt they were more effective.

What is your opinion on whether the existing laws related to cyber terrorism are sufficient to combat the issue in Bangladesh?



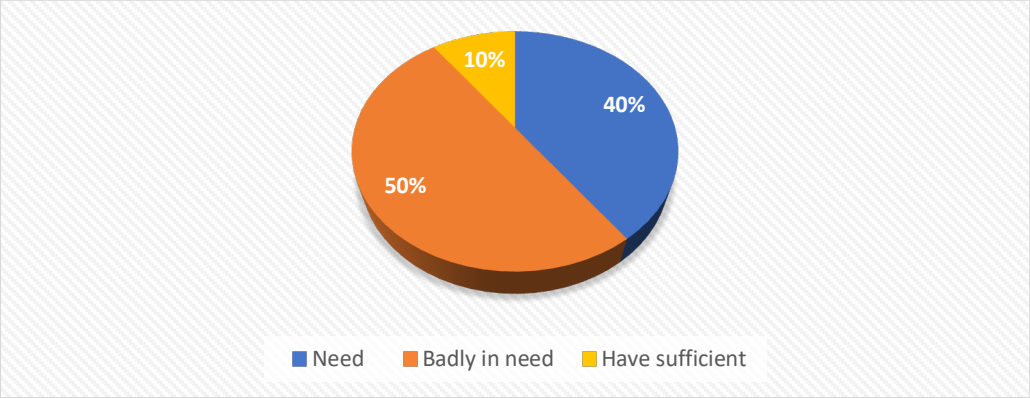
In response to this question, 50% of the total respondents indicated that new laws are needed to combat cyber terrorism. Meanwhile, 20% suggested amending existing laws, another 20% believed the current laws were sufficient, and 10% felt that the existing laws were not enough.

Is the current manpower of law enforcement agencies sufficient?



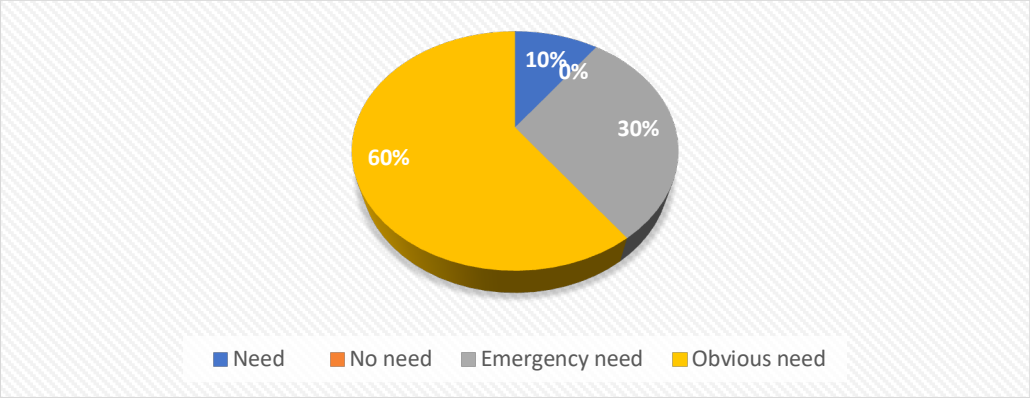
In response to this question, 40% of the total respondents indicated that the current manpower of law enforcement agencies is inadequate. Furthermore, 50% expressed the need for expert personnel, another 10% suggested increasing the overall number of staff, and 10% believed that the existing manpower was sufficient.

Do law enforcement agencies require any special equipment to prepare for combating cyber terrorism?



In response to this question, 50% of the total respondents stated that there is a critical need for special equipment to combat cyber-terrorism. Additionally, 40% indicated that such equipment is needed, while 10% felt that the current resources are sufficient to protect against cyber terrorism in Bangladesh.

Do law enforcement agencies require any special technical expertise to prepare for combating cyber terrorism?



In response to this question, 60% of the total respondents indicated that special technical expertise is needed to combat cyber terrorism. Additionally, 30% expressed that there is an urgent need for such expertise, while 10% stated that it is obviously necessary to address cyberterrorism in Bangladesh.

4.2 In-depth Interview

The interviews aimed to identify various challenges faced by law enforcement officials in fulfilling their responsibilities related to cyber terrorism in Bangladesh. Insights were gathered from Assistant Superintendents of Police (ASP) in the Counter Terrorism Unit and Anti-Terrorism Unit, as well as from Officers-in-Charge at the district level to understand current preparedness against cyber terrorism. Officials provided feedback on key areas, offering a realistic view of the agency's capabilities.

Interview with ASP of Counter Terrorism Unit

Questions were asked across multiple aspects to achieve the research objectives. Officials provided the following insights:

a. Existing laws are not fully adequate to combat cyber terrorism, highlighting the need for new legislation or amendments to current laws.

b. There is a need for expert personnel with specialized knowledge in cybercrime.

c. Enhanced cooperation with developed countries is essential for strengthening counter-cyber terrorism efforts.

Interview with ASP of Anti-Terrorism Unit

Through similar questions, officials shared a candid view of their agency’s current capabilities:

i. Officers have received training from the Cyber Police Centre in Bangladesh, the Indian Cyber Intelligence Unit, and the Jordan Cyber Crime Division. They emphasized that extending cooperation with the U.S. government would be beneficial for combating cyber terrorism.

ii. Officials advocated for the creation of specific laws addressing cyber-terrorism.

iii. Strengthening coordination with other domestic agencies actively involved in counter-cyber terrorism was noted as critical.

Interviews with Officers-in-Charge at the District Level in Khulna

To understand district-level preparedness, the researcher interviewed three Officer-in-Charge in the Khulna district. They noted that there is currently no effective mechanism in place for countering cyber terrorism at the district level.

5. Discussion

The current capability of law enforcement agencies to combat cyber terrorism in Bangladesh falls short of meeting the growing challenges. Their limited efficiency is further constrained by numerous barriers, including insufficient expertise, outdated legal frameworks, and inadequate resources. These obstacles not only hinder effective response to cyber threats but also emphasize the urgent need for improved training, modernized equipment, and stronger legal support to effectively counter cyber terrorism.

5.1 Challenges that stand in the way

Availability of information

The vast availability of information on the internet, with millions of constantly updated webpages, allows anyone who publishes or maintains a site to participate in the digital space. This extensive accessibility makes it challenging for law enforcement agencies to secure cyberspace against cyber terrorism, as the abundance of readily available information can be exploited by malicious actors.

Missing mechanism of control

The lack of centralized control mechanisms poses a significant challenge in managing mass communication networks, from phone networks used for calls to the Internet. These networks require centralized administration and technical standards to ensure they function smoothly. Similarly, the Internet needs governance through clear laws, prompting lawmakers and law enforcement agencies to establish legal standards that introduce a necessary level of centralized oversight.

Cross-border dimensions

The international nature of data transfer processes often spans multiple countries, as internet

protocols rely on optimal routing. When direct pathways are temporarily blocked, data can still flow across international borders. Even with limitations on domestic transfers in the source country, information can exit the country, pass through routers in foreign territories, and return to reach its final destination. This complexity adds a layer of difficulty for national regulations and monitoring, emphasizing the need for cross-border cooperation in cybersecurity efforts.

Location independence in cybercrime

Cybercriminals can operate remotely, often far from the physical location of their targets, making many cyber offenses inherently transnational. This separation complicates investigations and enforcement, as cybercrime frequently spans multiple jurisdictions and requires extensive coordination and resources. Additionally, cybercriminals often avoid countries with robust cybercrime laws, seeking out "safe havens" where legislation is weaker. Eliminating these safe havens remains a crucial challenge in the global fight against cybercrime.

Rapid data exchange

Data transfer across countries occurs in mere seconds, exemplified by the instantaneous nature of email, which has transformed communication by eliminating the need for physical message delivery. While this speed is a cornerstone of the internet's success, it poses a significant challenge for law enforcement agencies. The brief window for data exchange leaves minimal time to investigate or gather evidence, as traditional investigative methods require much more time to respond effectively to cyber incidents.

Traditional Investigative Tools

Addressing cyber-terrorism demands internet-specific tools and techniques that equip authorities to conduct effective investigations. While some instruments overlap with those used in conventional terrorism cases, traditional investigative methods increasingly fall short in internet-related incidents. In many cyber cases, these tools cannot trace and identify offenders, underscoring the need for specialized digital investigative resources to combat cyber terrorism effectively.

5.2 Recommendations for advancing the status of the LEAs

To counter cyber terrorism effectively, strategic plans must be established to ensure the security of the nation and its citizens. The following recommendations outline key areas for enhancing the capabilities of Bangladeshi law enforcement agencies to tackle cyber threats:

Develop and Implement Security Best Practices: Law enforcement agencies should create and deploy customized security best practices tailored to their operations. Implementing these measures requires coordinated efforts across all departments, as adherence to security procedures is essential organization-wide.

Proactive Cyber Security Measures: Agencies should adopt a proactive stance on cyber terrorism by keeping up-to-date on the latest threats, vulnerabilities, and incidents. This commitment to ongoing improvement will strengthen their information security readiness.

Multi-Level Security Architecture: Improving existing security infrastructure by deploying multi-tiered security architectures, rather than single-tier systems, will provide better protection against cyber threats.

Encouraging the Use of Security Applications: The use of firewalls, Intrusion Detection Systems (IDS), anti-virus software, and other security applications should be promoted and, where needed, mandated for enhanced cyber protection.

Comprehensive Network and Activity Monitoring: Deploying both network-based and host-based IDS, along with other security applications, can greatly enhance monitoring. Designated personnel should be assigned to log, observe, and report all suspicious activities, leveraging advanced security systems for efficiency.

Retention of Forensic Information: Ensuring the preservation of critical information needed for forensic analysis will support ongoing and future investigations into cyber incidents.

Collaboration with Public and Private Bodies: Law enforcement agencies and the public should establish working relationships with both public and private entities. These partnerships can support the development of security guidelines, disaster recovery plans, and discussions on emerging cyber-terrorism issues.

Expert Knowledge Exchange: Regular information exchange with experts in cyber-terrorism will create a vital resource pool, enhancing general resilience against cyber-attacks.

Strengthened Cyber Laws: The government should adopt and revise cyber laws to introduce heavier penalties for cyber terrorism and encourage the development of efficient cybersecurity practices. Enabling law enforcement to access more effective tools through legal support is also essential.

National Law Adjustments: Adjusting national laws to address the misuse of new technologies is vital, starting with the recognition of such abuses.

Addressing Encryption Challenges: Encryption technology, while key for data protection, can hinder cybercrime investigations. Law enforcement should develop methods to address these challenges effectively.

Alignment of Legal Provisions with New Offenses: Legislative foundations should be periodically assessed to ensure alignment with emerging cybercrime offenses.

Integration of Digital Evidence: With the increasing use of ICTs, digital evidence has become crucial in legal proceedings. The shift toward digitization impacts evidence collection and usage, making it essential for agencies to adapt to this development.

6. Concluding Remarks

Although many of us are relatively new to the field of cyberterrorism, it is undoubtedly a complex and challenging area. Across the globe, significant progress has been made in defending against cyber-attacks due to the collaborative efforts of industry and government initiatives. It's widely recognized that security is not a one-time solution; rather, it's an ongoing journey requiring continuous commitment from all involved. Protecting against cyber terrorism involves understanding the different motivations and types of attacks, grasping the impact these attacks have on critical infrastructure, businesses, and individuals, and implementing often intricate strategies to minimize risks.

The challenge is substantial, but with well-planned security measures and stronger collaboration across various sectors—industry, government, and the public—we stand a solid chance of combating these threats effectively. The reality is that cyberterrorism will persist,

and there is still much work ahead to fully protect nations, industries, and individual interests. However, the good news is that with the strategic plans already in place, we are progressively moving toward our ultimate goal: a highly secure, resilient, and productive environment for all.

The role of law enforcement agencies (LEAs) in this regard is paramount, as they are tasked with detecting, preventing, and investigating cyber-related crimes. These agencies must stay ahead of evolving threats by continuously updating their skills and technologies, collaborating with international partners, and fostering public awareness about cybersecurity. By building strong networks and information-sharing systems, LEAs can enhance their effectiveness in tackling cyber-terrorism, ensuring that they are prepared to respond swiftly and efficiently to any incidents that may arise. Ultimately, their proactive engagement and commitment to innovation will play a critical role in safeguarding communities from the pervasive threat of cyber-terrorism.

References

Awati R, Sheldon R and Hanna KT, 'What Is Cyberterrorism?' (*Tech Target*) <https://www.techtarget.com/searchsecurity/definition/cyberterrorism> accessed 2 November 2024

'Background' (*Anti Terrorism Unit, Bangladesh Police*) <https://atu.police.gov.bd/about-us/> accessed 2 November 2024

'Bangladesh Cyber Threat Landscape 2022' (BGD e-GOV CIRT) <https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/publications/effc311d_5097_46ba_afa4_5f44b60a93e6/Bangladesh%20Cyber%20Threat%20Landscape%202022.pdf>

Byron RK and Rahman MF, 'Bangladesh Bank Cyber Hacking: The Billion-Dollar Hit Job' *The Daily Star* (4 February 2020) <https://www.thedailystar.net/business/banking/bangladesh-bank-cyber-hacking-billion-dollar-hit-job-1863310> accessed 2 November 2024

'Cyber Attacks Hit over 200 Organizations Including Bangladesh Bank, BTRC' *Dhaka Tribune* (2 April 2021) <https://www.dhakatribune.com/bangladesh/242875/cyber-attacks-hit-over-200-organizations-including> accessed 2 November 2024

'Cyber Police Center' (*Criminal Investigation Department | Bangladesh Police*) <https://www.cid.gov.bd/public> accessed 2 November 2024

'Cyber Terrorism' (*Wigan Council*) <https://www.wigan.gov.uk/Resident/Crime-Emergencies/Counter-terrorism/Cyber-terrorism.aspx> accessed 2 November 2024

'Definition of CYBERTERRORISM' (*Merriam-Webster*) <https://www.merriam-webster.com/dictionary/cyberterrorism> accessed 2 November 2024

Maruf A, Islam MR and Ahamed B, 'Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies' (2014) 1 Northern University Journal of Law

'Police Cyber Support For Women' (*Bangladesh Police*) <https://www.police.gov.bd/en/police_cyber_support_for_women> accessed 2 November

2024

'Towards Developing a Counter-Terrorism Policy for Bangladesh' (Bangladesh Enterprise Institute) <http://bei-bd.org/wp-content/uploads/2015/04/Towards-Developing-a-Counter-Terrorism-Policy-for-Bangladesh.pdf>