ISSN: 1683-8475

NDC JOURNAL

VOLUME 23 NUMBER 2 FEBRUARY 2025

A Professional Journal of National Defence College
Bangladesh


“Read! In the name of your Lord Who has created (all that exists)”
Surah Al-Alaq (Verse 96)

NDC JOURNAL
Security Through Knowledge

A Professional Journal of National Defence College, Bangladesh

Volume 23 | Number 2 | February 2025

National Defence College
Bangladesh

DISCLAIMER

Published by the National Defence College, Bangladesh

Design & Printed by: Ornate Care
70/2, Nayapaltan, Dhaka-1000, Bangladesh
Cell: 01911546613, E mail: ornatecare@gmail.com

NDC JOURNAL
Security Through Knowledge

CONTENTS

	Page
Message from the Chief Patron	v
Editorial	vi
Abstracts	vii
Analysis of Digital Transformation in the Financial Sector and Need for Secure Information Technology (IT) Architecture to Protect Against Cyber Threats Brigadier General Kazi Mustafizur Rahman, SPP, ndc, psc	01
A Critical Analysis of Bangladesh Cybersecurity Strategy: Challenges and Ways Forward Brigadier General Raisul Islam, SPP, ndc, afwc, psc	29
The Emergence of a Fluid Multipolarity: Challenges and Opportunities for Bangladesh National Security Air Commodore Md. Zahir Uddin, GUP, ndc, acsc, psc, GD(P)	49
Climate Change and Regional Security: Challenges for West Africa Captain Musa Danjuma Jarma, ndc	73
The Impact of Social Media in Shaping Military Public Opinion in Oman Group Captain Rashid Hamdan Said Al Kalbani, ndc	95
Indigenous Defence Industry through Reverse Engineering: A Drive towards Self-sufficiency for Bangladesh Army Colonel K M Mehedi Hasan, afwc, psc	113
Quest for a Sustainable Knowledge Management Architecture: Optimising Existing Research-Based Knowledge of Bangladesh Armed Forces Lieutenant Colonel Quzi Md Nahidul Islam, SUP, afwc, psc, Infantry	133

Impact of 4IR Technology on Naval Warfare: Challenges for Bangladesh Navy and Ways Forward 157
Commander Mahbuba Afroze, (L), afwc, psc, BN

Unmanned Aerial Vehicle in Warfare: Challenges in Airspace Management in Bangladesh 179
Group Captain Salah Uddin Md Alim-Al-Rabbi, GUP, afwc, psc, GD(P)

University-Industry Collaboration for Development of Aviation Industry in Bangladesh: Challenges and Way Forward 201
Group Captain Sk Ashraful Hossain, afwc, psc, GD(P)

An Analysis of the Command and Control System Following the Transition of Leadership from "Generation X" to "Generation Z": Bangladesh Armed Forces Perspective 223
Colonel S M Moniruzzaman, SGP, afwc, psc

Eco-Tourism as a Catalyst for Sustainable Development in the South-West Region of Bangladesh 239
Lieutenant Colonel G M Mamunur Rashid, psc, G+, Air Defence

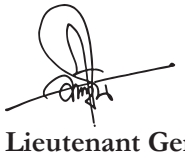
MESSAGE FROM THE CHIEF PATRON

It gives me great pleasure to introduce this journal from the National Defence College, which stands as a testament to our enduring commitment to excellence in leadership, defense, security, strategy, and development studies. Since its establishment in 1999, the National Defence College has remained committed in its mission to serve as the premier national centre of academic excellence, addressing the multifaceted challenges of the 21st century.

Within these pages, readers will find a collection of research papers that exemplify the dedication and intellectual rigor of our Course Members and Faculty. These papers cover a diverse array of topics, which are of utmost importance to our nation's security and development. Through original insights and analysis, our contributors demonstrated their deep understanding of contemporary issues and their implications on both national and international scale.

I would like to extend my heartfelt congratulations to all the authors whose works are showcased in this journal. Your contributions reflect the culmination of rigorous research and thoughtful analysis, and I have no doubt that they will prove invaluable to readers seeking to deepen their understanding of critical issues facing our world today. Besides, my gratitude to the Research and Academic Wing for their unwavering dedication to fostering a culture of intellectual inquiry and scholarly excellence at the National Defence College. I also commend the editorial board for their diligence and commitment in bringing this journal to fruition.

Finally, as we continue to navigate the complexities of the modern world, it is imperative that we remain steadfast in our pursuit of knowledge and understanding. I am confident that the insights presented in this journal will contribute significantly to our collective efforts to address the challenges and opportunities that lie ahead.



Lieutenant General Mohammad Shaheenul Haque
Commandant
National Defence College

EDITORIAL

National Defence College, Bangladesh is the premier national centre of excellence in leadership, Security, Strategy and Development Studies. The College believes that a senior officer from the military and civil services should have a good understanding of the major economic, political and social issues of the nation and be able to recommend measures to meet the challenges. Hence, NDC regularly conducts various research works on contemporary issues of national as well as international importance.

NDC Journal is a bi-annual publication of the National Defence College, publishing selected research papers prepared by the Course Members. The articles for the journal (Volume 23, Number 2, February 2025) are primarily selected from individual research papers that the Course Members had submitted as part of the course curricula. National Defence College publishes the 'NDC Journal' every year. This speaks of the laborious effort and genuine commitment on the part of both the editorial staff and the writers.

A total of 12 (twelve) Research Papers have been adjudged for publication in the current issue in abridged form. The articles reflect complex and intricate multidimensional issues emanating from the long, diversified experience of the course members and the curriculum-based deliberations and discourse on various topics concerning comprehensive national security during the training. This volume includes papers of different categories that will be able to draw the attention of varied groups of readers.

We would like to express our sincere gratitude to the Chief Patron, Lieutenant General Mohammad Shaheenul Haque, OSP, BSP, ndc, hdmc, psc the Commandant of NDC, for his valuable guidance. As we all know, research is a highly committed undertaking. Despite all efforts, unintentional errors in various forms may appear in the journal. We ardently request our valued readers to pardon us for such unnoticed slights and shall consider ourselves rewarded to receive any evocative criticism. We hope that all papers included in this volume will be able to satisfy our readers.

Md Badrul Amin
Air Vice Marshal (LPR)
Editor-in-Chief

ABSTRACTS

ANALYSIS OF DIGITAL TRANSFORMATION IN THE FINANCIAL SECTOR AND NEED FOR SECURE INFORMATION TECHNOLOGY (IT) ARCHITECTURE TO PROTECT AGAINST CYBER THREATS

Brigadier General Kazi Mustafizur Rahman, SPP, ndc, psc

The financial sector's growing dependence on technology has made it more vulnerable to cyber-attack. This study aims to examine how digital transformation affects the financial sector and emphasizes the need for secure IT architecture to mitigate cyber threats, identify key cyber threat categories and their potential effects, assess the effectiveness of current IT security architecture against cyber risks, and propose defensive IT architecture for secure digital financial management. Employing a blend of quantitative and qualitative data collection methods, this study proposes the adoption of "Zero Trust Architecture". Overall, the study provides valuable insights on secure IT architecture and recommendations to enhance the cybersecurity of Financial Organization of Bangladesh.

Keywords: Digital Transformation, Cyber Security Framework, Secure IT Architecture, Zero Trust Architecture.

A CRITICAL ANALYSIS OF BANGLADESH CYBERSECURITY STRATEGY: CHALLENGES AND WAYS FORWARD

Brigadier General Raisul Islam, SPP, ndc, afwc, psc

In the age of growing cyber insecurities, no nation, whether powerful or weak, big or small, developed or developing, is immune to cyber threats. Developing countries with relatively weak surveillance capacity are most vulnerable to such threats. The effectiveness of a nation's cybersecurity lies in its strategy, typically aligned with International Telecommunication Union (ITU) standards. This study assesses the effectiveness of the 'Bangladesh Cybersecurity Strategy 2021-2025,' the official document delineating the country's cybersecurity measures. The country has invested commendable efforts in strengthening its digital infrastructure and protecting its citizens, businesses, and organizations from cyber threats. However, a critical analysis of the strategy reveals for improvement in adherence with the standard structure of ITU along with concise vision and time bound implementation plan, ensuring a comprehensive legal framework with effective enforcement, effective skill development with standalone R&D capabilities, and enhancing effective international cooperation and collaborations.

Concluding remarks are followed by policy recommendations to address urgent issues and contemporize Bangladesh's cybersecurity readiness promptly.

Keywords: Cybersecurity Strategy, Cybersecurity of Bangladesh, Cybersecurity Strategy Formulation Approach, Challenges of Bangladesh Cybersecurity Strategy and Ways Forwards of Bangladesh Cybersecurity.

THE EMERGENCE OF A FLUID MULTIPOLARITY: CHALLENGES AND OPPORTUNITIES FOR BANGLADESH NATIONAL SECURITY

Air Commodore Md. Zahir Uddin, GUP, ndc, acsc, psc, GD(P)

Bangladesh's remarkable rise to one of the fastest-growing economies in the world has brought the country to a crucial geopolitical position. Currently, the world is transforming towards multipolar world, where power and influence are shifting globally. The study examines how fluid multipolarity, the changing power dynamics among global and regional actors, affects Bangladesh's security and economic ties. It identifies opportunities and challenges for Bangladesh in this complex landscape and suggests foreign policy guidelines to achieve its goals. These include a non-partisan foreign policy, friendly relations with all nations, active regional and multilateral engagement, humanitarian diplomacy, climate adaptation, and sustainable development. The study uses a qualitative approach and relevant data. It argues that Bangladesh must safeguard its interests and promote global peace through a vigilant and proactive approach to international relations.

Keywords: Geopolitical Position, Fluid Multipolarity, Power Dynamics, National Security, International Relations.

CLIMATE CHANGE AND REGIONAL SECURITY: CHALLENGES FOR WEST AFRICA

Captain Musa Danjuma Jarma, ndc

Climate change is changing security landscapes around the world. Unfortunately, studies have shown that West Africa is experiencing climate change at rates faster than the global average, which is magnified by the region's low resilience, hence the spate of insecurity. Unfortunately, insecurity in West Africa has largely been associated with local politics. While this research concedes the previous, the impact of climate change as a security threat multiplier in West Africa underscores

a refocus on its impact at the local, national, and regional levels with a view to proffering ways of tackling its security-related challenges, which forms the crux of this study.

Keywords: Climate Change, Regional Security, Climate Change-related Security Challenges.

THE IMPACT OF SOCIAL MEDIA IN SHAPING MILITARY PUBLIC OPINION IN OMAN

Group Captain Rashid Hamdan Said Al Kalbani, ndc

In the contemporary period characterized by the widespread presence of various social media platforms, it is of utmost importance to comprehend their impact on military public opinion. The present study examined the complex interplay between social media platforms and the shaping of military public opinion within the context of Oman. The study identified primary determinants that contribute to this influence and examined how these determinants shape the viewpoints and dispositions of both military personnel and civilians towards the Omani military. This study aimed to examine the influence of social media on the formation of public opinion inside the military, with a specific focus on the Omani military. By analyzing this relationship, significant insights can be gained on the development of efficient communication and messaging strategies within the Omani military setting. The results of the study indicated that social media has a significant impact on the formation of military public opinion, as it functions as a versatile medium for the sharing of information, discourse, and engagement. The scope of this influence encompasses both individuals serving in the military and the wider civilian population, exerting an effect on their perspectives and opinions pertaining to subjects relating to the military. Significantly, social media platforms possess the capability to strengthen prevailing beliefs, question established conceptions, and provide opportunities to engage with a wide range of opinions. This study provided valuable insights into the dynamic influence of social media on the formation of military public opinion, hence presenting practical recommendations for improving communication methods within the military environment of Oman.

Keywords: Social Media, Military Public Opinion, Military Environment, Oman.

INDIGENOUS DEFENCE INDUSTRY THROUGH REVERSE ENGINEERING: A DRIVE TOWARDS SELF-SUFFICIENCY FOR BANGLADESH ARMY

Colonel K M Mehedi Hasan, afwc, psc

Excessive import dependency on defence items has both economic and security concerns. Given the geo-strategic reality, the Bangladesh Army should be self-reliant on its essential hardware and ammunition. However, establishing technology-ridden defence industries, where Research and Development (R&D) makes the difference, remains elusive for most developing countries like Bangladesh. In that context, Reverse Engineering can be an alternative perspective. Reverse Engineering, a technology of reinvention through measuring, analyzing, and testing to rebuild the mirror image of an object, may become a road map leading to indigenous defence production for the Bangladesh Army. This research initially identified the need for a self-reliant army in the context of geo-political realities followed by the options and methods available for the Bangladesh Army for indigenization. The paper then checked the viability of Reverse Engineering in four dimensions: Legal, Economic, Technological, and Infrastructural. Eventually, the challenges and ways forward for Reverse Engineering are identified. A probable road map is also furnished at the end.

Keywords: Reverse Engineering, Indigenization, Self-reliance, Technology Transfer, Joint Venture.

QUEST FOR A SUSTAINABLE KNOWLEDGE MANAGEMENT ARCHITECTURE: OPTIMISING EXISTING RESEARCH-BASED KNOWLEDGE OF BANGLADESH ARMED FORCES

Lieutenant Colonel Quzi Md Nahidul Islam, SUP, afwc, psc, Infantry

This thesis explores knowledge management (KM) practices within the Bangladesh Armed Forces (BDAF), emphasising its significance within the organisation. The study reveals that despite BDAF's annual contribution to research-based knowledge (RBK), a lack of sustainable KM infrastructure hinders the efficient utilisation of RBK. This deficiency leads to knowledge redundancy, data loss, and difficulties sharing, storing, and retrieving information. To overcome these obstacles, the study proposes developing a tailored KM architecture that can leverage BDAF's vast and diverse RBK to foster innovation. The research analyses various KM models, including SECI, Bukowitz & Williams, McIntyre, Tiwana, and Wiig, and

provides a comprehensive knowledge-sharing and utilisation framework. This framework aims to optimise existing RBK, enhance organisational performance, and promote innovation.

Moreover, the study emphasises that a sustainable KM architecture can effectively manage and apply an organisation's knowledge assets. This architecture comprises a clearly defined knowledge strategy, promoting a culture of knowledge exchange and collaboration, establishing a robust infrastructure, and implementing KM initiative evaluation metrics. By integrating sustainable KM into all organisational processes, the study finds that human capital's knowledge and performance can be improved. However, the study also identifies several challenges to implementing KM, including technology limitations, cultural norms, limited resources, organisational complexities, information security concerns, and resistance to change. The study suggests that BDAF adopts a new KM system architecture that combines the McIntyre (2003) and Tiwana (2002) models to address these challenges. This approach aims to manage RBK and prevent duplication of efforts effectively. Ultimately, the paper concludes that overcoming these challenges and implementing an effective KM system in BDAF can maximise intellectual resources, enhance organisational outcomes, and foster innovation.

Keywords: Knowledge Management, Research-Based Knowledge, Knowledge Management Architecture, Knowledge Management Cycle, Knowledge Management System.

IMPACT OF 4IR TECHNOLOGY ON NAVAL WARFARE: CHALLENGES FOR BANGLADESH NAVY AND WAYS FORWARD

Commander Mahbuba Afroze, (L), afwc, psc, BN

The advent of the 4th Industrial Revolution, characterized by the integration of emerging technologies such as artificial intelligence, robotics, big data analytics, and the Internet of Things, has disrupted various sectors of society, including the realm of warfare. This research paper examines the profound impact of the 4th Industrial Revolution on naval warfare and explores the challenges it poses to naval forces, specifically focusing on the implications for the Navy. The paper begins by providing an overview of the key technologies driving the 4th Industrial Revolution and their potential applications in the naval domain. It discusses the increasing role of particularly Artificial Intelligence and Big Data Analysis in naval operations, including surveillance, reconnaissance, and even offensive capabilities. It delves into the integration of big data analytics and

machine learning algorithms for enhanced decision-making, target identification, and threat detection. Furthermore, the study investigates the challenges that naval forces face as a result of the 4th Industrial Revolution. These challenges encompass not only technological advancements but also ethical, legal and operational considerations. The paper addresses the challenges and the need for adapting naval strategies by Bangladesh Navy to exploit the advantages provided by AI and Big Data. In light of these challenges, the research paper presents a range of proposed strategies, roadmap and recommendations for BN to overcome the hurdles posed by the 4IR. The utilisation of AI in contemporary combat is exemplified by the deployment of drones, UAVs and other similar technologies and its unprecedented outcomes in the Nagorno-Karabakh Conflict and Ukraine War. Israel, Turkey and Iran have risen as AI Super Power and enabled them to be considered as power house of such technology. By embracing AI and Big Data while simultaneously addressing the associated challenges, Bangladesh Navy can effectively optimize the combat capabilities.

Keywords: 4th Industrial Revolution, Artificial Intelligence, Big Data Analysis, Strategy and Roadmap for BN, Optimize the Combat Capabilities.

UNMANNED AERIAL VEHICLE IN WARFARE: CHALLENGES IN AIRSPACE MANAGEMENT IN BANGLADESH

Group Captain Salah Uddin Md Alim-Al-Rabbi, GUP, afwc, psc, GD(P)

Unmanned Aerial Vehicle (UAV) has revolutionized military operations by offering significant advantages such as increased situational awareness, reduced risk to human personnel, extend operational reach, and enable rapid response capabilities which help commanders in decision making process. Bangladesh Armed Forces (BDAF) have also started operating UAV in the congested airspace of Bangladesh (BD) which is likely to pose challenges and threats to airspace management (ASM). At this backdrop, the broad objective of this research is to find out the challenges and threats to ASM of BD for employment of UAV to its full capabilities, and to propose mitigation measures to address them. This is an exploratory type of research and followed qualitative methodology using primary and secondary data. At the very outset, potential capabilities of UAV are identified analyzing the recent wars. Subsequently, ASM policies, regulations, circulations of Civil Aviation Authority of BD (CAAB) as well as selected countries were studied to find out the challenges like detection capability of radar, limited airspace of BD, UAV operations from busy airfield, separation between the UAV and manned aircraft, technical failure of UAV etc, and threats like illegal surveillance and reconnaissance, smuggling, mid-air collision etc to ASM of BD. To address the

challenges and threats, mitigation measures are proposed. BD needs to establish comprehensive regulatory frameworks for UAV operations, including operational guidelines and ensuring safety to manned aircraft. Additionally, investment in advanced surveillance and detection systems would enable effective monitoring and controlling of UAV activities. Above all a holistic approach is necessary for formulating appropriate rules and regulations and executing UAV operations effectively with its full capabilities in airspace of BD.

Keywords: Unmanned Aerial Vehicle, Airspace Management, Challenges, Threats and its Mitigation.

UNIVERSITY-INDUSTRY COLLABORATION FOR DEVELOPMENT OF AVIATION INDUSTRY IN BANGLADESH: CHALLENGES AND WAY FORWARD

Group Captain Sk Ashraful Hossain, afwc, psc, GD(P)

The aviation industry is expanding faster over the world and there is acute shortage of skilled manpower in this sector. Aviation industry in Bangladesh (BD) has acute shortage for both Operational and Non-operational (Back-office) professional. Thereby, its being compelled to hire foreign professional and incurred loss of foreign exchange. Bangabandhu Sheikh Mujibur Rahman Aviation and Aerospace University (BSMRAAU) as the first public university of BD of its nature, generates mainly operational aviation professional. BSMRAAU has been incorporating most of the Civil Aviation Authority of BD (CAAB) accredited curriculum including AME in their syllabus. To meet the acute shortage of skilled manpower and resource sharing, worldwide University-Industry Collaboration (UIC) has been introduced in aviation sector. Through UIC, both university and aviation industry gets benefited in terms of developing skilled manpower, research product, internship, and finally employment. In that note, BSMRAAU has a bright prospect of collaboration with BD aviation industry with the support of CAAB. BD gadget also authorised BSMRAAU to affiliate with all aviation and aerospace institutes of BD. Objective of this study is to find out whether formidable UIC (considering BSMRAAU) can generate required skilled manpower for BD aviation industry or not. For effective and successful UIC in BD aviation industry, few challenges are identified. However, with a formidable UIC plan, BSMRAAU is likely to overcome these challenges successfully and generate required aviation professionals for BD aviation industry.

Keywords: Civil Aviation Authority of Bangladesh, Aviation Industry, University-Industry Collaboration, Skilled Manpower

AN ANALYSIS OF THE COMMAND AND CONTROL SYSTEM FOLLOWING THE TRANSITION OF LEADERSHIP FROM "GENERATION X" TO "GENERATION Z": BANGLADESH ARMED FORCES PERSPECTIVE

Colonel S M Moniruzzaman, SGP, afwc, psc

The Bangladesh Armed Forces are currently led by members of Generation X, who have experience in both the analog and digital eras, while the majority of their subordinates are from Generation Z, who were born in the digital era. As is true in all facets of society, there is a synchronization gap between these two generations. However, this difference is anticipated to disappear once the members of Generation Z are in command of the Bangladesh Armed Forces. But as digitalization continues to evolve, they likely will experience transformations in the command and control system. The advantages of automated decision-making, communication between soldiers on the front lines and the highest headquarters, lowering risks to human soldiers, saving human hours, network-centric warfare, automated soldiers' psychological assessments, etc. would result from technological advancement. Making sensible and calculated decisions is necessary to reduce the possibility that technology innovation may limit tactical commanders' initiative, lead to a reduction in manpower, compromise the security of military data, etc.

Keywords: Generation X, Generation Z, Digitalization, Technology, Transformation, Command and Control.

ECO-TOURISM AS A CATALYST FOR SUSTAINABLE DEVELOPMENT IN THE SOUTH-WEST REGION OF BANGLADESH

Lieutenant Colonel G M Mamunur Rashid, psc, G+, Air Defence

Eco-tourism has been recognised as a transformative force to bring about sustainable development around the world, especially for developing countries like Bangladesh. This study examines the present eco-tourism situation, evaluates the potential benefits, and identifies the critical challenges of eco-tourism from economic, social, and environmental perspectives to ensure sustainable development in the south-west region of Bangladesh. A mixed-method approach has been applied combining qualitative and quantitative data collected from secondary and primary sources. The study revealed that the current situation of eco-tourism in the south-west region is less developed despite of its immense

potential. Also, eco-tourism has the capacity to contribute for the welfare of the society, economic growth and environmental conservation, thereby supporting successful sustainable development in the region. However, critical challenges such as insufficient infrastructures, inadequate framework and policy, lack of community involvement, limited promotion, and financial constraints hinder eco-tourism in the region. To maximise benefits and overcome challenges, measures such as a co-management approach, integrated eco-tourism policies, sufficient infrastructures, and effective economic, social, and environmental strategies are recommended. Thus, eco-tourism can be utilized as a catalyst for sustainable development in the south-west region of Bangladesh.

Keywords: Eco-tourism, Sustainable Tourism, Sustainable Development, South-west Region.

NDC JOURNAL
Security Through Knowledge

ANALYSIS OF DIGITAL TRANSFORMATION IN THE FINANCIAL SECTOR AND NEED FOR SECURE INFORMATION TECHNOLOGY (IT) ARCHITECTURE TO PROTECT AGAINST CYBER THREATS

Brigadier General Kazi Mustafizur Rahman, SPP, ndc, psc

Introduction

Digital transformation (DT) may defined as "a product, process, or business model that is perceived as new, requires some significant changes on the part of adopters, and is embodied in or enabled by Information Technology (IT)" (Dos Santos, Fichman and Zheng, 2014). The intersection of finance and IT is referred to as Digital Finance or Fintech, which encompasses the digitization of the financial sector (Gomber, Koch and Siering, 2017). In the financial domain, this process encompasses utilizing digital tools like mobile banking, internet banking, blockchain, artificial intelligence (AI), and more to enhance operational efficiency, customer satisfaction, and overall profitability. The fourth industrial revolution is marked by the widespread adoption of digital technologies, the Internet, and social networks, among other things, making it an era of DT that holds significant promise for sustainability due to its vast potential (Roblek et al., 2020).

In recent times, the financial sector in Bangladesh has experienced substantial expansion due to the rise of digital technologies. The Central Bank of Bangladesh (BB) has been a critical driver of DT initiatives in the financial domain, promoting digital technologies to upgrade financial services, increase financial inclusion, and reduce financial crime. For the past few years, Bangladesh has made remarkable progress in creating a cashless economy and achieving widespread financial inclusion. (Kamal, 2022).

Despite potential advantages, there are still several obstacles and constraints to DT in the financial sector in Bangladesh. These encompasses security concern and cyber-crime, establishing trust & rapport and heightened competition. The other challenges include limited digital infrastructure, low levels of digital literacy among the population, and apprehension regarding data privacy and security. As the volume of digital payments rises substantially, the vulnerability to cybersecurity threats like phishing, virus attacks, and malware is also rising. A study indicates that worldwide card fraud losses are projected to surpass $35 billion in the year 2020. (Kamal, 2022).

In February 2016, cyber attack in Bangladesh Babk SWIFT system served as a stark reminder to the financial industry that they had significantly undervalued the systemic cyber threats (Maurer and Nelson, 2021). Therefore, the objective of this study is to examine and explore how DT affects the financial sector and to recognize the necessity for a robust IT architecture to guard against cybersecurity risks, with the ultimate goal of providing recommendations for enhancing the IT security architecture of Financial Organizations (FOs).

Problem Statement

Cyber threats are constantly evolving, and FOs must keep up with the latest threats and vulnerabilities to protect themselves from attack. Cyberattacks can lead to monetary setbacks, harm to reputation, and legal responsibility for FOs. A secure IT architecture is essential to ensure business continuity and protect against the potentially catastrophic consequences of a cyberattack. The significance of the problem for the research lies in the need for FOs to address the growing cybersecurity risks associated with DT and to implement a secure IT architecture to protect against cyber threats.

Research Objectives

- To analyze the DT in the financial domain and its impact on the security of financial data.
- To identify the categories of cyber threats encountered by the financial sector and their potential impact on FOs.
- To evaluate the effectiveness of current IT security architecture in protecting against cyber threats in the financial sector.
- To suggest defensive IT architecture to mitigate these threats and secure digital financial management.

Principal Research Question. What is the impact of DT on the need for secure IT architecture to protect against cyber threats in the financial sector?

Literature Review

Azarenkova et al., (2018) highlighted that the integration of financial technologies has increased complexity in the global financial system. It proposed measures to address this include global norms, revised Financial Institute (FI) licensing, and legal frameworks for digital tokens (Azarenkova et al., 2018).

Mavlutova et al., 2023 explored how DT, particularly through innovative technologies like digital payments, contributes to the sustainable advancement of the financial domain. It provides valuable insights for future research and practical recommendations for professionals involved in the DT of the financial domain to support its sustainability (Mavlutova et al., 2023).

Dr. S. Amudhan, 2022 aimed to examine the socioeconomic attributes of participants designated from the study region. Digital banking significantly affects rural customers (Dr. S. Amudhan, 2022).

Bahl, 2012 acknowledged that Electronic banking, also known as e-banking, is the future trend, offering significant advantages to consumers in terms of transaction convenience and affordability (Bahl, 2012).

Ozili, 2018 explores the influence of electronic economy on inclusive finance and stability. It suggests that E-finance, particularly through Fintech firms, has a favorable impact on inclusive finance in both developing and developed economies (Ozili, 2018).

Doerr et al., (2022) highlighted that Cyber-threats in the financial domain are a growing risk to steadiness. This paper reports survey results on cyber risk in central banks, revealing heightened security investments since 2020 (Doerr et al., 2022).

Research Methodology

Research Method

The qualitative method used to gather data from the participants through in-depth interviews, Focused Group Discussion (FGD), Key Informant Interview (KII) and case studies. The quantitative method used to collect data through surveys, questionnaires, and data analysis to measure the impact of DT on the financial domain, the level of cybersecurity preparations by the FOs, and the effectiveness of secure IT architecture. To collect the data, the researcher has used a combination of online questionnaires, FGD, KII, and analysis of existing data, depending on the types of research questions and the population of interest.

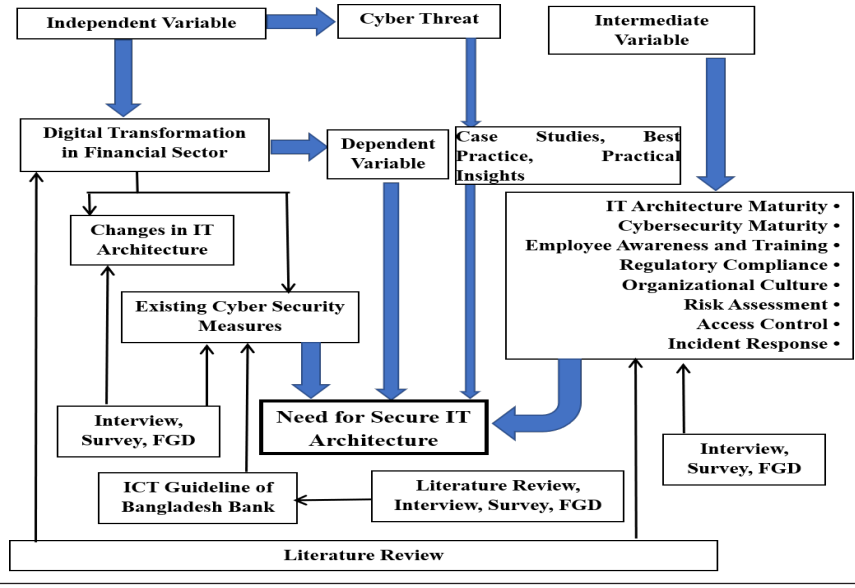
Data Sources

Primary data is collected through interviews, survey questionnaires, and discussions with various stakeholders, including cybersecurity experts, financial institution representatives, Bangladesh Bank representatives, bank account holders, ethical hackers, IT experts within banks, managing directors, board of directors, subject matter experts, academics, researchers,

and security professionals among others. Secondary data is sourced from literature, including books, research articles, journals, newspapers, websites, and social media ensuring a comprehensive and well-rounded dataset for analysis.

Conceptual Framework

Figure 1: Conceptual Framework



Source: Researcher

Digital Transformation in Financial Sector of Bangladesh and Its Impact

Financial System of Bangladesh

The Bangladesh financial system comprises three sectors: Formal, Semi-Formal, and Informal. Across the previous twenty years, Bangladeshi financial institutes especially banks, have made substantial investments in ICT, to enhance their information and communication productivity, efficiency, profitability, and competitive edge.

DT in the Financial Sector of Bangladesh

The growing FinTech ecosystem in Bangladesh presents untapped opportunities, with the global FinTech Market projected to reach 32 trillion USD by 2026. Bangladesh's improving infrastructure readiness in areas like electricity, mobile networks, e-governance, and digital services sets the stage for sustainable growth (The Business Standard, 2022).

Transformed Electronic Banking Operations

The Impact of DT. Over the past two decades, Bangladesh's banking sector has undergone a significant shift from manual to electronic banking (Source: BIBM Survey).

- **Online Banking.** As of March 2023, all Bangladeshi banks operate exclusively through 11,167 online branches. Table-1 reflects that 100% of Banks in Bangladesh are within online coverage and the state of transformation of offline branches to online branches.

Table 1: Online Branches of Bangladeshi Bank

Type of Bank	Total Branches	No. of Branches Online Coverage	Percent of Online Branches
SOCBs	4235	4235	100%
SDBs	1468	1468	100%
PCBs	4918	4918	100%
FCBs	66	66	100%
Total	10687	10687	100%

Source: BB Financial Stability Report 2021, Issue 12

- **Mobile Banking.** Bangladesh has become a digitally advanced nation by successfully implementing bank-led Mobile Financial Services (MFS) through modern technological advancements and increased mobile phone usage. Bangladesh is one of the most rapidly-expanding mobile money markets in the globe (Ahmed, 2019). Due to growth of MFC, in March 2023, approximately 198 million MFS account holders conducted a total of 482 million transactions, amounting to 1.08 trillion taka.
- **Plastic Card (Debit, Credit and Prepaid).** The growth of the use of debit, credit and prepaid cards, their transaction and transaction amounts are increasing at a high rate in Bangladesh.
- **SMS Banking.** Approximately 96% of banks in our country provide SMS banking services to their customers.
- **Digital Remittance.** As forecasted in Figure-19, by 2027, the projected total amount is estimated to be US$258.30m of digital remittance (Digital Remittances - Bangladesh | Statista Market Forecast, 2023).

Technologies Used in Financial Sectors

Digital technologies are pivotal in driving DT. When these technologies are integrated with effective business strategies, they can propel a company toward digitalization. The rise of cutting-edge technologies are Industrial 4.0, Block Chain, Artificial Intelligence (AI) and Machine Learning (ML), Crypto Currency, e-KYC (Electronic Know Your Customer).

Impact of DT on the Financial Sector of Bangladesh

DT has enabled greater financial inclusion by making financial services more accessible to underserved and marginalized populations. It has helped FOs in Bangladesh to streamline their processes, reduce operational costs, and improve efficiency by automating many of the manual processes. DT has enabled FOs in Bangladesh to provide a more seamless, personalized, and convenient customer experience. It also has enabled FOs in Bangladesh

to enhance transparency and security by leveraging blockchain and other distributed ledger technologies. DT has driven innovation and growth in the financial sector of Bangladesh, facilitating the creation of novel financial offerings.

Table 2: Effects of DT in the Financial Institutes

Changes in the Organizational Setup	Changes in Economics	Spillovers creating changes on other levels of analysis
Permeable, agile organizational structures	Improved firm performance and new forms of value	Higher exposure to cyber threats
Technology-focused and supported management	Dynamic and constantly changing industry level performances	Digital-permeated markets, economics and societies
Digital and customer experience-focused business model		Blurring boundaries between physical and online industry structures
Automatized, data-driven and virtual business processes		Digitalization of the individual
Smart, connected and customized products		Paradigms of customer-centricity and connected markets
Ecosystem-oriented and embedded organization		

Source: Researcher

Challenges of DT in the Financial Sector of Bangladesh

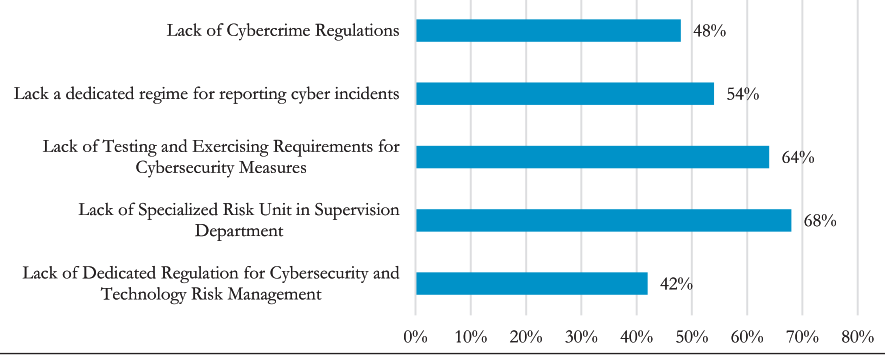
While DT offers many benefits to the financial sector of Bangladesh, it also presents several challenges that need to be addressed. Despite significant progress in recent years, Bangladesh still faces challenges in terms of digital infrastructure security. As digital payments continue to surge, the susceptibility to cybersecurity threats like phishing, virus attacks or malware, is also on the rise (Kamal, 2022). DT has created new regulatory challenges for FOs in Bangladesh, particularly in terms of compliance with data protection and privacy laws. Many people in Bangladesh lack the digital literacy skill and driving digital and financial literacy is crucial for users to comprehend and adopt services effectively (Kamal, 2022).

Overview of Cyber Threat in Financial Sector and Study of Existing IT Architecture

Global Cyber Threat Landscape

The Global Cybersecurity Index report highlights global cybersecurity legislation and regulations, emphasizing privacy and unauthorized access. It emphasizes the importance of capacity building in governments and businesses to address evolving cyber risks. A recent IMF survey across 51 countries found that many financial supervisors in emerging markets lack cybersecurity regulations and resources for enforcement. The survey indicates gaps, with a significant percentage lacking a national cyber strategy (56%), dedicated regulations for cybersecurity (42%), and a specialized risk unit (68%). Related lacks are shown in Figure-2.

Figure 2: Lack of Cybersecurity Regulations and Establishment



Source: Researcher

Bangladesh Cyber Threat Landscape

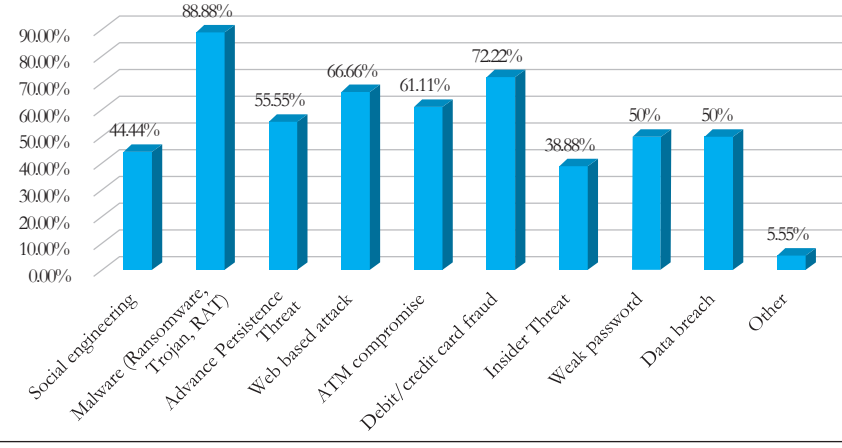
Bangladesh, like other nations, is not immune to the effects of global cyber warfare, experiencing its fair share of threat alerts and cybersecurity challenges (Rahman and Hussain, 2022). The 2016 incident in Bangladesh served as a critical moment for central banks and financial authorities worldwide, alerting them to the evolving threat landscape where certain risks could potentially pose systemic implications (Nelson, 2020). As of

April 23, 2019, there were reports of the Silence Group carrying out cyberattacks against FOs in the UK, India, and South Korea. The attacks had been ongoing since the end of 2018 and resulted in theft from at least one institution.

Threat Analysis in the Financial Sector of Bangladesh

Categories of Cyber Threats Encountered by the FOs. The survey conducted among 18 FOs in Bangladesh highlights the diverse spectrum of cyber threats faced by this sector. The data indicates that a significant number of financial organizations grapple with various forms of cyberattacks. Malware, encompassing threats like Ransomware, Trojans, and Remote Access Trojans (RATs), is the most prevalent, affecting 88.88% out of the 18 organizations surveyed. Details of other categories of cyber threats is shown in Figure-3.

Figure 3: Categories of Cyber Threat Encountered by the FOs (%)



Source: Survey Result

Banks Embracing Cyber Security Solutions

54% of banks reported having a dedicated Computer Incident Response Team (CIRT). Table-3 illustrates the utilization of various security solutions by the banks, with weak implementation observed for Security Operation

Center (SOC), API Security, Security Orchestration, Automation and Response (SOAR), identity and access management (IAM), and dynamic access management (DAM).

Table 3: Security Solutions by Bank

Types of Security Services / Solutions	% of Bank
SOC	54
SIEM	75
API Security	43
PAM (Privilege Access Management)	60
SOAR	27
IAM	5
DAM	24

Source: Survey Result

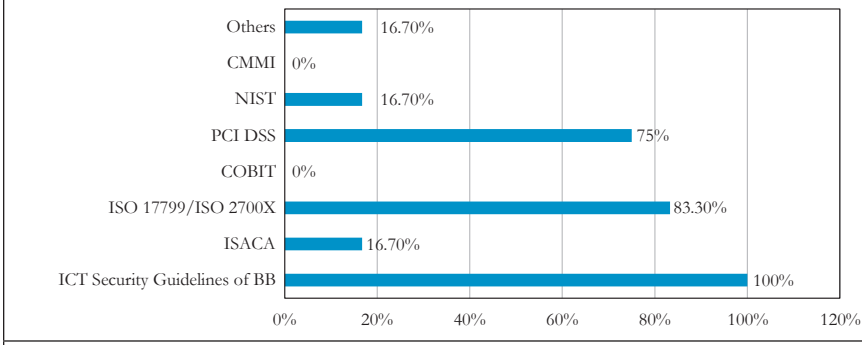
Cybersecurity Regulations, Frameworks and Compliance Standards for Banks

Adopting sustainable tech, robust security measures, skill enhancement, and strategic resource allocation can address cybersecurity challenges. The Bangladesh Bank's "Guideline on ICT Security Version 4.0" provides updated details, aligning with supervisory expectations. All financial organizations surveyed (100%) adhere to BB ICT Guidelines.

Cybersecurity Frameworks (CSF)

From a survey point of view, all banks are compliant with BB ICT Security Guidelines. Additionally, 83% of banks have adopted ISO 27001, while Payment Card Industry Data Security Standard (PCI-DSS) is being followed by 75%. Figure-4 gives idea on use of security framework by FOs of Bangladesh.

Figure 4: Use of IT Security Framework



Source: Survey Result

Global Certifications

Survey shows that 61.5% of banks secure PCI-DSS compliance for e-card data security. 53% attain ISO 27001:2013, 13% ISO 9001, and 10% Tier certification (Survey Report).

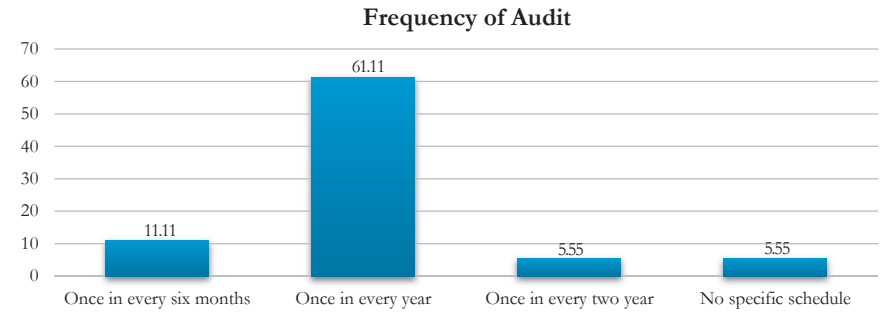
Use of Two Factor Authentication (2FA) and 3D Secure 2.0 Version by Banks in E-commerce

According to survey, 92.3% banks use two factor authentications (2FA) for doing E-commerce transactions like Online Merchant Payment, Utility Bill payments etc. Among them, 67% banks use 3DS version 2.0 for E-commerce transactions, 33% banks do not use this technology (Researcher Survey).

IT Audit

Approximately 84% of FOs have 1 to 8 dedicated IT Auditors, 16% lack an IT Audit team. Only 55% of auditors are internationally certified.

Figure 5: Information and System Audit State



Source: Survey Result

Penetration Testing (PT)

88% of banks in our country conduct penetration tests, with 22.22% annually, 50% half yearly, and 11.11% after significant network changes. (Details in Figure-6). More than 85% of banks rely on third-party vendors Over 85% of banks outsource penetration tests; 28% use in-house experts with consultant support (Field Survey).

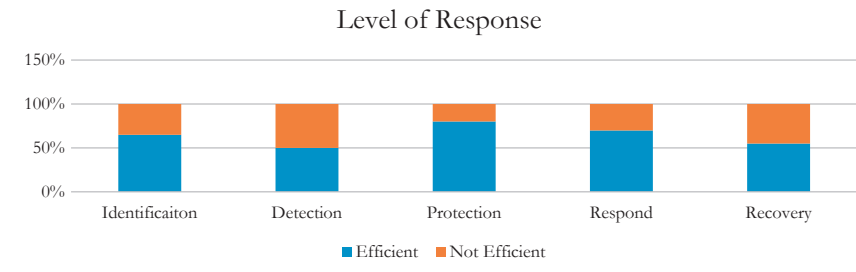
IT Risk Management

47% of banks have a dedicated IT Risk Management department, employing 2 to 15 people (average 7). 38% employ certified security professionals, averaging 8.5. About 73% have a dedicated security management unit (Survey Report).

Level of Response to Cyber Attack

According to the survey, the level of response to the 05 (five) pillars of cybersecurity by the FO is shown in figure 6:

Figure 6: Level of Response to Cybersecurity Pillars

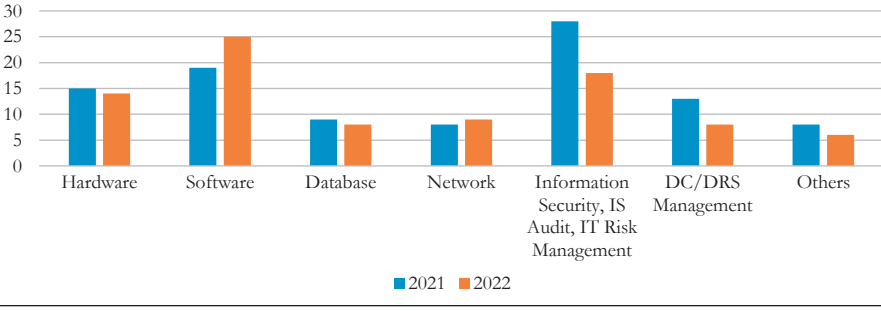


Source: Survey

IT Security Training

Figure-7 illustrates the percentage of IT employees who received training in different IT areas in 2021 and 2022. 66% bank opined that due to shortage of fund regular training cannot be provided.

Figure 7: IT Security Training Provided by Banks (% of IT Employment)

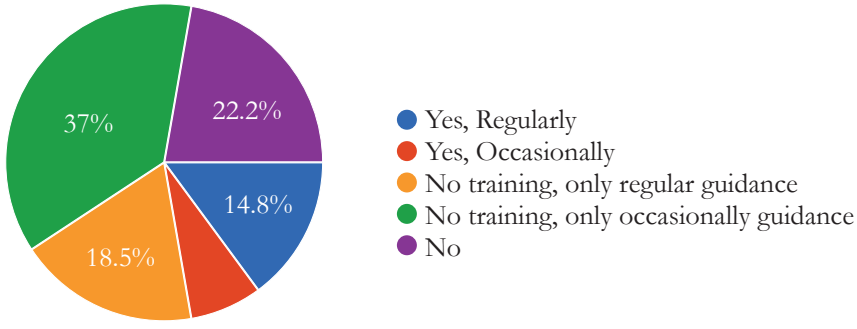


Source: Survey Result

Awareness Training of Employees and the Customer

Only 37% of customers receive occasional cybersecurity guidance; 42% never change passwords willingly; 66% trust banks' protection efforts; 15% lack sufficient cyber-attack alerts. Detailed are shown in figure 8.

Figure 8: State of Training/Guidance for the Customers of Banks



Source: Researcher Survey

Overview of Existing IT Architecture of the Financial Sector in Bangladesh

Core Banking System (CBS). Currently, there is a decline in banks opting for joint-venture CBS, with only 5.41% of banks using it in 2022, down from 11% in 2021. Conversely, there is an increasing adoption of in-house CBS by banks, with over 16% using it in 2022, up from 7% in 2021.

Data Center (DC). 2% of banks use Tier-2 and Tier-3 data centers; only 3% have Tier-4, impacting robustness.

Disaster Recovery Site (DRS). In 2020, 90% of banks had a Near DC (NDC), and 35% had Far DCs (FDC), showing improvement from 2019. (BIBM Survey).

Status of Hot DR in Banks. In 2022, active NDCs increased to 48% (from 42% in 2020), but only 24% FDCs are active.

Implementation of Security Control. Only 61% of banks have Host Intrusion Prevention System (HIPS), and 76.9% have encryption facilities.

Facts of Existing IT Architecture. Research findings reveal weaknesses in the IT system, detailed in Table-4.

Table 4: Findings on Existing IT Architecture of FOs

Serial	Findings	% of FO/Respondent
1	Consideration of IT expenditure as cost center is barrier for expenditure on cyber security	66.66%
2	There is a lack of expertise on exercising best practices of cyber security	55.55%
3	The cost of security products is high which is a barrier for cybersecurity solutions	94.44%
4	FO allot less budget for cybersecurity product	66.66%
5	There is a lack of information sharing on breaches of cybersecurity	72.22.%
6	There is a drawback to the lack of awareness generation within employees for cyber security	72.22%
7	There is a lack of monitoring and strict compliance assessment by the BB on cyber/ICT security	33.33%
8	To protect the brand reputation most of the time cyber incidents are not reported	72.22%
9	Due to inadequate training IT team of the FO are not adequately qualified in cybersecurity	27.77%
10	Due to insufficient funding, regular training cannot be provided to the IT professionals of FO	33.337%

Source: Survey Result

Cyber Incident Protection Measures. Banks employ multiple security measures, with 47% regularly updating anti-malware, but progress falls below expectations.

Availability of Technologies and Practices. Table-5 depicts the state (%) of availability of different security technology measures in FOs.

Table 5: State (%) of availability of security technology

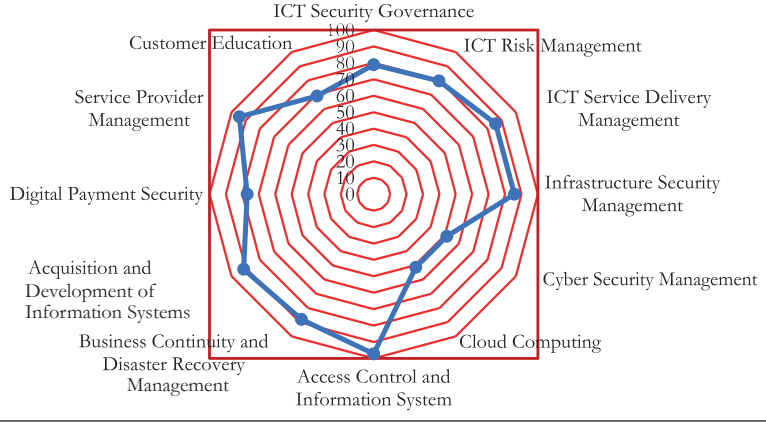
Technology and Practices	% of Bank
Endpoint Detection and Response (EDR)	90%
Data Loss Prevention (DLP)	22%
Security Information and Event Management (SIEM)	50%
Multi-Factor Authentication (MFA)	84%
PAM (Priviledge Access Management	61%
Continuous Security Training	50%
Blockchain Technology	40%
Cloud Security Solutions	55%
SOC	61%

Source: Survey Result

Overall Cybersecurity Gap Analysis in the FOs of Bangladesh

Based on survey data from 18 (eighteen) different FOs of Bangladesh, a gap analysis has been conducted to assess their current security state of ICT. The analysis utilized a scale of 100 points to evaluate various aspects as shown below and their graphical representation made in Figure-9.

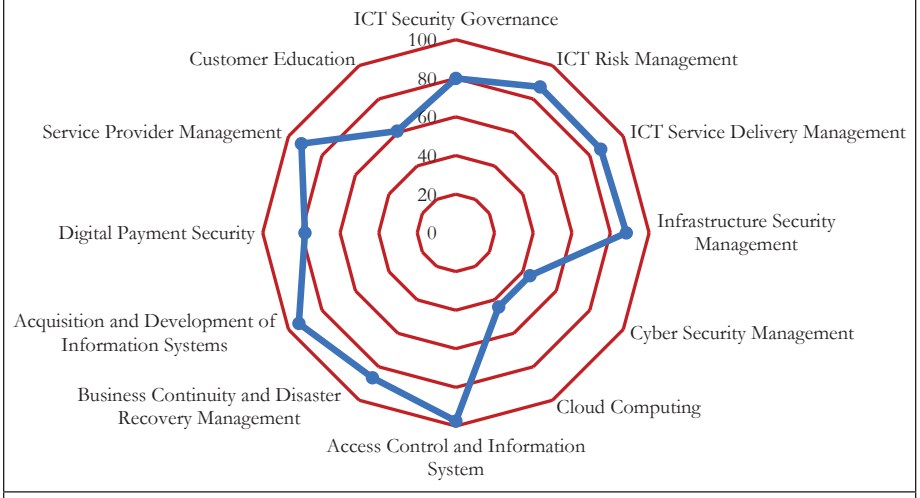
Figure 9: Cybersecurity Gap Analysis



Source: Researcher

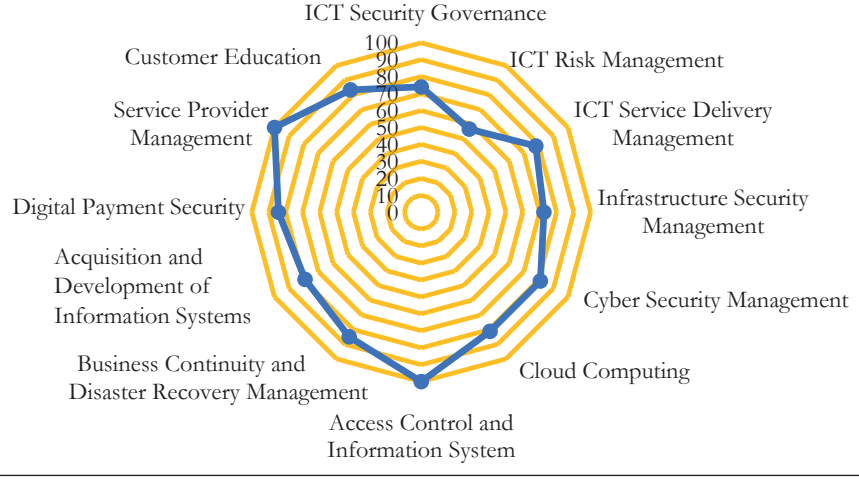
Cybersecurity Gap Analysis for Private Commercial Bank, State-owned Commercial Bank and Non-banking Financial Institutes are shown below:

Figure 10: Cybersecurity Gap Analysis on Private Commercial Banks



Source: Researcher

Figure 11: Cybersecurity Gap Analysis on State-owned Commercial Bank



Source: Researcher

Addressing the Need for Secure IT Architecture: A Suggested Design Approach

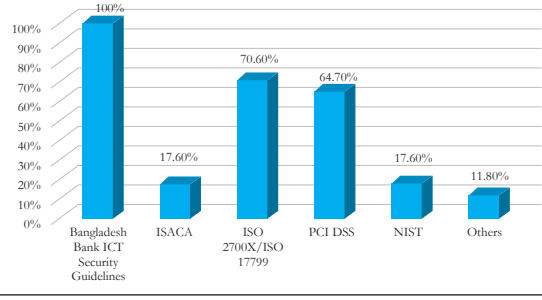
Overview of Cybersecurity Framework (CSF) and Security Architecture

A CSF comprises global standards and best practices aimed at safeguarding information and IT infrastructure from cyber-attacks and security threats. It encompasses rules, standards, practices, and concepts that ensure strong protection (Atoum, Otoom and Abu Ali, 2014). A security architects follow established guidelines or frameworks and create consistent guidelines and principles to implement security architecture. Organizations can choose to develop their own frameworks by combining international standards. (Security Architecture: What it is, Benefits and Frameworks, 2023). The NIST CSF consists of five main pillars: Identify, Protect, Detect, Respond, and Recover, making it suitable for businesses of all sizes and cybersecurity maturity levels. Major global organizations, including Microsoft, JP Morgan & Chase, and Intel, use this framework in their security programs.

Adoption of CSF by the FOs of Bangladesh

The survey reveals that each financial organization in Bangladesh has adopted various CSFs. It seems that many FOs blindly follow other people's footsteps without clearly understanding what they want to achieve. The recent data leakage demonstrated both the improper adoption and the absence of proper implementation of CSF (Dhaka Tribune, 2023).

Figure 12: Different CSF adopted by FO

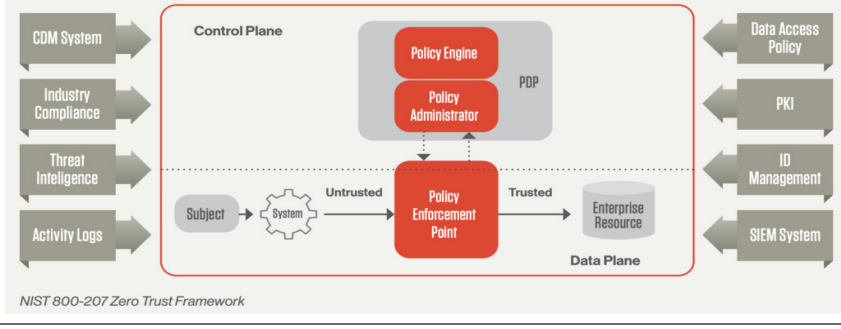


Source: Survey Result

Evolving Security Architectures

As per Section-3 of the "Executive Order on Improving the Nation's Cybersecurity" issued by the White House on May 12, 2021, the President of the United States directed the development of a Zero Trust Architecture (ZTA) plan. The plan emphasized including migration steps outlined by NIST and indicating completed steps, prioritizing activities with immediate security impact, and providing an implementation schedule (The White House, 2021).

Figure 13: NIST 800-207 Zero Trust Framework



Source: (What is Zero Trust Security? Principles of the Zero Trust Model, no date)

The Concept of ZTA

The traditional security model relies on perimeter security with the concept of "Trust but verify," trusting internal users but being cautious about external attacks. Table-6 presents the comparison between the traditional security model and the zero-trust model.

Table 6: Comparison between the traditional security model and the zero-trust model

Features	Traditional Security Model	Zero-Trust Model
Approach	Trust but verify	Trust nothing and verify everything
Trust Boundary	External (Non-trust), Internal (Trust)	Micro Segmentation
Access Control	IP (Port, Protocol) based access control	Data-centric access control
Communication Encryption	External (Encryption)/Internal (No Encryption)	Full traffic encryption
Authentication	Once verification at initial access	Before access and continuous verification
Security Policy	Pre-defined rules and common policies	Fine-grained rules and adaptive policies (Needs Security Assessment)
Security Management	Individual Monitoring and visibility	Visibility, automation orchestration of behaviour, devices, services and security

Source: Sarkar et al., 2022

Perspectives for New Architecture Apart from Traditional CSF

General. Traditional strong perimeters are inadequate in the digital age. Organizations must adopt a holistic approach to ensure continuous security, verifying every person and device accessing systems. This study advocates for a new defensive architecture for FOs in Bangladesh (As revealed from Focus Group Discussion).

Increased Cyberattacks. Organizations relying on single sign-on (SSO) may face risks; complementing it with Multi-factor Authentication (MFA) enhances security, and Zero Trust models further strengthen defense (Sreejith, 2022).

Risks of Flat Network Architecture. Organizations maintaining flat networks face security risks; Zero Trust architectures aim to address vulnerabilities, enhance security, and mitigate potential breaches (Aibangbee, 2022).

The Rise of Work From Home (WFH). Post-pandemic WFH increases security risks; Zero Trust Security, with strict access controls, addresses vulnerabilities in BYOD scenarios (Sreejith, 2022).

Opinion of Cybersecurity Experts. Surveyed cybersecurity experts in FOs favor ZTA; its tools align with BB's ICT Security Guidelines, facilitating infrastructure establishment.

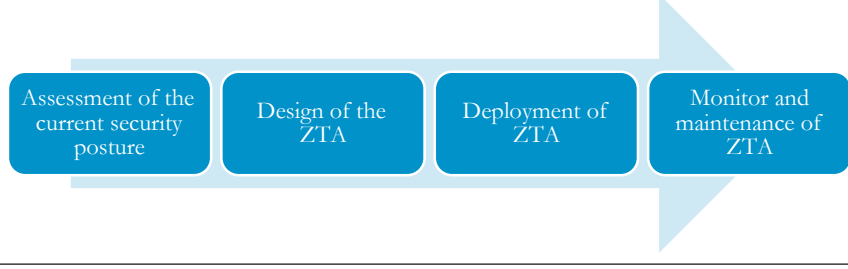
Enhancing Security: The Power of ZTA for FO

Adopting zero-trust helps FOs meet security requirements, protect customer data, and maintain customer trust (Frąckiewicz, 2023). FOs adopt zero-trust architecture for robust security amid reliance on digital systems. ZTA replaces traditional security with user/device authentication, reducing data breach risks. ZTA minimizes costs by eliminating traditional infrastructures, enhancing security and reducing breaches. Banks adopt zero-trust architecture for compliance, data protection, and enhanced security processes. Banks employ zero-trust architecture to combat fraud, requiring authentication for user and device access, ensuring security and mitigating threats (Frąckiewicz, 2023).

How to Achieve a ZTA

General. There are a number of ways and means to achieve ZTA in the Financial Organization of Bangladesh. Some of the key steps involved include:

Figure 14: ZTA Implementation Process



Source: Researcher

- **Implementing Micro-segmentation.** Smaller segments that isolate the network into small segments.
- **Using IAM.** For managing who has access to what resources.
- **Implementing MFA.** Adds an extra layer of security by requiring users to provide multiple pieces of evidence to prove their identity.
- **Using Security Information and Event Management (SIEM).** It collects and analyzes security logs from across the network

Challenges of Transition to ZTA

Firstly, stakeholders including top leadership, resist in ZTA Implementation. Secondly, overlooking access controls and security configurations can expose vulnerabilities in network segments. Thirdly, management's financial and operational support is vital for successful implementation. Additionally, ZTA is a complex architecture, and it can be difficult to implement and manage. ZTA can be expensive to implement, especially for large organizations.

Overcoming ZTA Implementation Challenges

Implement ZTA in a limited environment. Gain user buy-in. Utilize available tools to automate ZTA implementation and management, reducing complexity and costs.

Recommendations

- Embrace Digital Transformation (DT) Holistically.
- Strengthen Cybersecurity Measures.
- Establishing Separate Financial CIRT (FinCIRT).
- Enhance Digital Literacy.
- Implement Zero Trust Architecture.
- Adherence to the ICT Security Guidelines.

Conclusion

The research explored DT in the financial sector, noting industry evolution and significant growth in digital financial transactions, fostering financial inclusion and a cashless economy. Bangladesh's banking sector transformed with 11,167 online branches, providing virtual services and benefiting rural and SME sectors through mobile banking and payment technologies.

In Bangladesh's financial sector, adopting DT presents both benefits and challenges, including digital infrastructure limitations, cybersecurity risks, regulatory compliance complexities, digital literacy gaps, and resistance to change. Addressing these challenges is crucial for successful DT adoption. FOs in Bangladesh face various cyber threats, with malware (88.88%), debit/credit card fraud (72.22%), and web-based attacks (66.66%) being prevalent. Banks follow BB ICT Security Guidelines, with 83% adopting ISO 27001, 75% PCI-DSS, and 16% ISACA. IT audits pose challenges; 84% have dedicated auditors, and 16% rely on external or central bank auditors.

FOs face barriers: viewing IT as a cost center, lacking expertise, high costs, limited budgets, awareness, monitoring, incident reporting, and training insufficiency. Adoption of CSFs varies, often neglecting governance, risk management, and compliance.

US DoD and DISA introduced "Black Core" for security; White House endorses ZTA via NIST guidelines. A study finds 93% consider zero trust vital for organization security. In the evolving digital landscape, relying on strong perimeters is insufficient. This study advocates a holistic approach for Bangladeshi financial organizations to adopt ZTA.

Banking adopts Zero Trust Architecture (ZTA), rejecting default trust in users and devices. Authentication, authorization, and micro-segmentation enhance security against cyber threats and data breaches, replacing traditional perimeter-based security.

References

1. Ahmed, F.T. (2019) Digital financial services can transform Bangladesh, Prothomalo. Available at: https://en.prothomalo.com/opinion/Digital-financial-services-can-transform (Accessed: 6 April 2023).
2. Aibangbee, Y. (2022) 'Adaptive Trust: Zero Trust Architecture in a Financial Services Environment', Bank Policy Institute, 21 March. Available at: https://bpi.com/adaptive-trust-zero-trust-architecture-in-a-financial-services-environment/ (Accessed: 24 July 2023).
3. Aldasoro, I. et al. (2020) 'The drivers of cyber risk', Bank for International Settlements (BIS) Working Paper, No 865(May 2020). Available at: https://www.bis.org/publ/work865.htm (Accessed: 24 May 2023).
4. 'All about digital banking fraud prevention' (no date) NetGuardians. Available at: https://www.netguardians.ch/digital-banking-fraud/ (Accessed: 20 July 2023).
5. Atoum, I., Otoom, A. and Abu Ali, A. (2014) 'A holistic cyber security implementation framework', Information Management & Computer Security, 22(3), pp. 251–264. Available at: https://doi.org/10.1108/IMCS-02-2013-0014.
6. Azarenkova, G. et al. (2018) 'The influence of financial technologies on the global financial system stability', Investment Management and Financial Innovations, 15, pp. 229–238. Available at: https://doi.org/10.21511/imfi.15(4).2018.19.
7. 'Bangladesh Bank Financial Stability Report 2021' (no date). Available at: https://www.bb.org.bd//pub/annual/fsr/financial_stability_report2022.pdf (Accessed: 8 July 2023).
8. BTRC (no date a) Bangladesh Telecommunication Regulatory Commission (BTRC), Mobile Subscriber. Available at: https://btrc.portal.gov.bd/site/page/0ae188ae-146e-465c-8ed8-d76b7947b5dd (Accessed: 3 July 2023).

9. Cyber Risk Outlook 2018 (no date) Cambridge Judge Business School. Available at: https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyber-risk-outlook/cyber-risk-outlook-2018/ (Accessed: 19 July 2023).

10. Dhaka Tribune (2023) Has a massive data breach exposed personal info of 50m Bangladeshis?, Dhaka Tribune. Available at: https://www.dhakatribune.com/bangladesh/2023/07/08/massive-data-breach-exposes-personal-info-of-50m-bangladeshis (Accessed: 26 July 2023).

11. Doerr, S. et al. (2022) 'Cyber risk in central banking', Bank for International Settlements (BIS) Working Paper, No 1039(September 2022). Available at: https://www.bis.org/publ/work1039.htm (Accessed: 24 May 2023).

12. Dr. S.Amudhan, D.S.B. (2022) 'Impact of Digital Transformation of Banking Sector in Rural Areas', Journal of Positive School Psychology, 6(2), pp. 763–771.

13. Frąckiewicz, M. (2023) 'Zero-trust Architecture for Finance and Banking Industry', TS2 SPACE, 21 May. Available at: https://ts2.space/en/zero-trust-architecture-for-finance-and-banking-industry/ (Accessed: 24 July 2023).

14. Gomber, P., Koch, J.-A. and Siering, M. (2017) 'Digital Finance and Fintech: Current Research and Future Research Directions'. Rochester, NY. Available at: https://papers.ssrn.com/abstract=2928833 (Accessed: 2 May 2023).

15. Kyle, C. (2023) Top 10 Cybersecurity Frameworks for the Financial Industry | UpGuard. Available at: https://www.upguard.com/blog/top-cybersecurity-frameworks-finance (Accessed: 24 July 2023).

16. Maurer, T. and Nelson, A. (2021) The Global Cyber Threat to Financial Systems – IMF F&D, International Monitoring Fund (IMF). Available at: https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm (Accessed: 6 April 2023).

17. Mavlutova, I. et al. (2023) 'Digital Transformation as a Driver of the Financial Sector Sustainable Development: An Impact on Financial Inclusion and Operational Efficiency', Sustainability, 15(1), p. 207. Available at: https://doi.org/10.3390/su15010207.

18. Nelson, T.M., Arthur (2020) International Strategy to Better Protect the Financial System Against Cyber Threats, Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2020/11/18/international-strategy-to-better-protect-financial-system-against-cyber-threats-pub-83105 (Accessed: 20 April 2023).

19. Ozili, P.K. (2018) 'Impact of digital finance on financial inclusion and stability', Borsa Istanbul Review, 18(4), pp. 329–340. Available at: https://doi.org/10.1016/j.bir.2017.12.003.

20. Rahman, T. and Hussain, M.F. (2022) 'Bangladesh Cyber Threat Landscape 2022', BGD e-GOV CIRT Shop. Available at: https://shop.cirt.gov.bd/product/cyber-threat-landscap-2022/ (Accessed: 15 July 2023).

21. Rose, S. et al. (2020) Zero Trust Architecture. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-207.

22. Security Architecture: What it is, Benefits and Frameworks (2023). Available at: https://www.threatintelligence.com/blog/security-architecture (Accessed: 24 July 2023).

23. Sreejith (2022) Why Do Businesses Need Zero Trust Security?, Fingent Technology. Available at: https://www.fingent.com/blog/why-do-businesses-need-zero-trust-security/ (Accessed: 26 July 2023).

24. The White House, T.W. (2021) Executive Order on Improving the Nation's Cybersecurity, The White House. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (Accessed: 27 July 2023).

25. Timeline of Cyber Incidents Involving Financial Institutions (no date) Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org (Accessed: 20 July 2023).

26. What is Zero Trust Security? Principles of the Zero Trust Model (no date) crowdstrike.com. Available at: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/ (Accessed: 24 July 2023).

Author

Brigadier General Kazi Mustafizur Rahman, SPP, ndc, psc was commissioned into the Bangladesh Army on 16 June 1994 in the Corps of Signals. Over his distinguished career, he has held various command, staff, and instructional appointments. He has commanded a Static Signal Company, a Signal Battalion, and a United Nations Military Contingent in the Democratic Republic of Congo. His staff appointments include serving as General Staff Officer Grade-3 of a Signal Brigade, Brigade Major of an Infantry Brigade, Grade One Staff Officer, and Colonel General Staff at the Directorate General of Forces Intelligence (DGFI).

In the rank of Brigadier General, he has served as the Project Director of a technical capacity-building project at DGFI, as Director of the Information Technology (IT) Directorate at Army Headquarters, and as Director General of the Bangladesh Telecommunication Regulatory Commission (BTRC). Academically, Brigadier General Mustafiz holds a Master's in Business Administration (MBA) from Southeast University, Dhaka; a Master's in Defence Studies (MDS) from National University; and a Master's in Information and Communication Technology (MICT) from Bangladesh University of Professionals (BUP). He is also a PhD fellow, registered under BUP for the academic year 2022-23. Currently, Brigadier General Mustafiz commands the 86 Independent Signal Brigade at Dhaka Cantonment. He is happily married and blessed with one daughter.

NDC JOURNAL
Security Through Knowledge

A CRITICAL ANALYSIS OF BANGLADESH CYBERSECURITY STRATEGY: CHALLENGES AND WAYS FORWARD

Brigadier General Raisul Islam, SPP, ndc, afwc, psc

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it" -Stephane Nappo

Introduction

Cybersecurity plays a significant role in achieving resilient cyberspace for economic prosperity and credible defence (Whiting & Wiiliams, 2013). A cybersecurity strategy is a comprehensive and structured plan developed by an organisation, government, or entity to identify, assess, and mitigate potential cyber risks and threats to their digital assets, information systems, networks, and data. As a step towards firming up the cybersecurity, the Government of Bangladesh (GoB) has published 'Bangladesh Cybersecurity Strategy 2021-2025 (BCS 2021-2025, 2022)' in January 2022. Bangladesh is poised to introduce a cybersecurity strategy with the goal of establishing a secure cyberspace environment. This initiative aims to enhance resilience against the increasing threats posed by cyber-attacks, ensuring the safe operation of digital networks (Jasim, 2022).

In the era of cyber insecurities, no nation, whether strong or weak, big or small, developed or developing, is immune to cyberattack (Islam, 2021). Developing countries, with relatively weak surveillance capacity, are most vulnerable to such cyber-attacks" (Nation, 2011). Regrettably, the Government of Bangladesh (GoB) embraced digitalization in numerous sectors without giving due emphasis to information security and infrastructure development. As a result, the country has encountered numerous cyber-attacks ranging from its foreign ministry website to Critical Information Infrastructures (CIIs) like Bangladesh Bank (Islam,

2021). However, very insignificant attempts had been made to assess the strategic strength of the cybersecurity strategy of Bangladesh by performing cross-comparisons with the standard and guidance of the International Telecommunication Union (ITU), a specialised UN agency for ICT. Therefore, the study aims to evaluate the effectiveness of the 'Bangladesh Cybersecurity Strategy 2021-2025' in a cross-comparison with the international standard set by the ITU and the best practices of different advanced countries with a view to developing a resilient and effective cybersecurity strategy for Bangladesh.

This study seeks to address the primary question, how effective is the existing cybersecurity strategy of Bangladesh for achieving a resilient cyber environment? To address the research query, this study employs a qualitative research approach, encompassing both primary and secondary data analysis. Moreover, thirteen cybersecurity experts were selected as key informants for in-depth interviews. Through these interviews, a more comprehensive understanding emerged regarding how the cybersecurity strategy functions, intervenes, and intersects with national security agendas. The purpose of this study is to suggest policy recommendations to fix the pressing issues of BCS 2021-2025 and improve the cybersecurity preparedness of the country in a timely manner. The findings of this research will assist the strategy developers to focus on the critical issues that will hinder the country's cybersecurity with a view to taking appropriate steps to negate the challenges.

Cybersecurity Environment of Bangladesh

Cyber Landscape of Bangladesh. Cybersecurity has emerged as a critical challenge for Bangladesh, as the country faces increasing cyber threats from internal and external actors. Bangladesh's total population was 172.1 million in January 2023, of which 40% lived in urban areas and 60% in rural areas (Kepios, 2023). Bangladesh's internet subscribers reached 123.82 million at the end of December 2021, 71.95% of the total population. Of which 113.73 million were using mobile internet

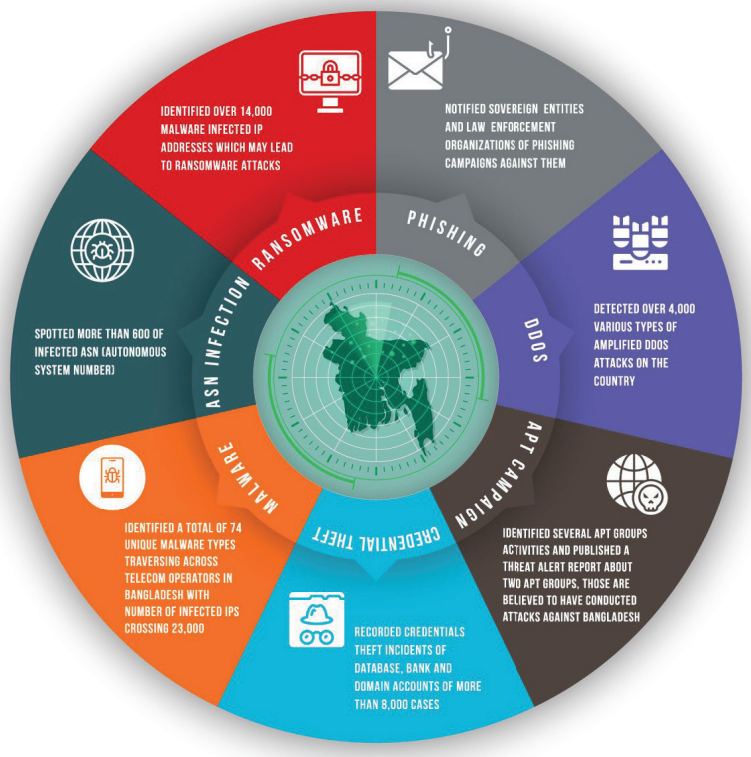
and 10.09 million broadband internet (BTRC, 2023). In January 2023, there were 44.70 million social media users in Bangladesh, 26.0% of the total population. According to Mr Shyam Sunder Sikder, Chairman of Bangladesh Telecommunication Regulatory Commission (BTRC), the internet bandwidth use in the country has increased from 7.5 Gbps in 2008 to 3,850 Gbps in 2022, which is 513 times (8FYP, 2020). The e-commerce market in Bangladesh is rapidly growing, with a market size of around 2.2 billion USD in 2021, projected to reach 8.6 billion USD in 2025. More than 25000 Government domains, 260 applications, 417 VPN file servers, 109 managed services, and 18059 network services have been hosted in the national data center by Bangladesh Computer Council (BCC, 2023).

Despite enormous progress in the cyber realm, the general mass of the country has limited knowledge on how to handle personal information in online and the protection issue of personal information. Many participants viewed social media as a national security risk because sites like Facebook and Instagram are thought to have been frequently used to spread false information. In a survey question regarding cybersecurity awareness, seventy-two percent of participants agreed that the common mass of the country is ignorant about cybersecurity. Sixty-nine percent of participants also stated that promoting cybersecurity awareness is deemed necessary to build a resilient cyber environment in the country.

Cyber Threat Landscape of Bangladesh. Bangladesh's cybersecurity is becoming more complex due to the repercussions of current geopolitical issues. The global economy began to recover from the devastating effects of the pandemic but was once again embroiled by the conflicts in Europe and Middle East. The conflicts also have a spill-over effect in global cyberspace. Threat actors like activists, hacker groups, and nation-states use destructive malware causing disruption and repercussions to global IT networks and infrastructures. Bangladesh is also experiencing the consequences of global cyberwarfare, as the Bangladesh Government's e-Government Computer Incident Response Team (BGD e-GOV CIRT) has identified unique cyber-attacks targeting Bangladesh's government,

financial, military, industrial, trade and commerce, healthcare, and energy sectors (CIRT, 2023). The country's detailed 'Cyber Threat Landscape-2022' is shown in Figure 1.

Figure 1: Cyber Threat Landscape 2022



Source: Bangladesh Cyber Threat Landscape 2022

According to the findings of interviews, internet users in Bangladesh blindly trust ICT and internet services and do not have the necessary skills to evaluate the security of their used applications. The trust level of e-commerce services has increased unprecedently due to the quality of service experienced since inception. On the contrary, the vendors of e-commerce services have not yet recognised the importance of application security despite frequent proliferation. The interviews revealed that the

BGD e-GOV CIRT and the police are the only channels for reporting online fraud, online child abuse, cyberbullying, identity theft, privacy, and security breach-related incidents.

Organisational Structure of Cybersecurity in Bangladesh. The organisational structure of cybersecurity in Bangladesh involves multiple agencies and organisations working together to protect the country's Critical Information Infrastructures (CIIs) and defend against cyber threats. In Bangladesh, the Ministry of Posts, Telecommunications and Information Technology (MoPT) is the apex organisation for cybersecurity. The ICT Division of MoPT is wholly responsible for cybersecurity issues. The ICT Division was detached from the 'Science and Technology Ministry' and reformed as the 'Ministry of Information and Communication Technology' in 04 December 2011 (ICT_Division, 2023). The development demonstrates that top-level policymakers recognise the value of ICT and that the government is eager to keep up with the pace of the rapidly changing modern world. Again in 2014, the 'Ministry of Information and Communication Technology' was integrated with the MoPT as an ICT Division (MoPT, 2023). Currently, most of the stakeholders of ICT are functioning under the directives and supervision of the ICT Division of MoPT. It encounters numerous challenges in serving as a dedicated focal point organization for cyber and ICT issues.

Legislative Structure of Cybersecurity in Bangladesh. GoB has enacted various cyber legislations, policies, and guidelines to fight against cybercrime. The ICT Acts 2006, 2009, 2013 (amendment), Digital Security Act 2018, Bangladesh Telecommunication Act 2001, 2006, 2010 (amendment), Anti-pornography Act 2012, National ICT Police 2018, and Digital Security Policy 2020 are the main legislative measures to deal with cybercrime in Bangladesh. Even after the government's enormous initiative, it is not being possible to effectively enforce the cyber law due to limited knowledge of law enforcement agencies and judiciary on ICT and cyber. However, critics argued that the existing legal measures in Bangladesh may fall short of achieving its goals. There are concerns

about potential infringements on freedom of expression, privacy rights, due process, and the lack of clarity and enforcement mechanisms within the legal framework.

Assessment of Bangladesh's Cybersecurity Strategy. The ICT Division of the MoPT published the 'National Cybersecurity Strategy 2014' in March 2014 with a stated goal of "working collaboratively at home and abroad, to manage all major cyber risks that affect us directly irrespective of their origin and type, thereby creating a safe, secure and resilient critical national information infrastructure for our economy and society" (NCS, 2014). The Digital Security Agency (DSA) under the ICT Division of MoPT published the 'Bangladesh Cybersecurity Strategy 2021-2025' in January 2022. The strategy is formulated based on the four pillars i.e., digital government, human resource development, industry promotion, and connecting citizens (BCS 2021-2025, 2022).

Bangladesh is set to roll out a cybersecurity strategy to foster the circumstances for the secure operation of the internet by strengthening resilience against the escalating risks of cyberattacks. Bangladesh Cybersecurity Strategy 2021-2025 has been developed based on four pillars but lacks in determining its comprehensive vision, goals, and time-bound implementation plan. Based on the interview results, it lacks a clear definition of priorities, resources, and implementation plans. Furthermore, not all its provisions can be implemented within the specified timeframe. The survey indicates a lack of coordination among the stakeholders engaged in its implementation.

According to the BCS 2021-2022, all ministries will be equipped with secured software and a skilled workforce to protect their information from cyber-attacks. However, the majority of ministries are not cognizant of the situation and have yet to commence the implementation process. Most of the KIIs opined that the adoption and implementation of controls in government bodies are insufficient and inconsistent. Most ministries' security controls are restricted to password protection and the use of

antivirus software only. Most of the stakeholders acknowledged that the cybersecurity strategy and policy-making process rests with the ministry only, and they have limited things to do. An inventory of software used in the public and private sectors and a catalogue of secure software are currently absent in Bangladesh despite the country having established a dedicated branch for ICT sector standardisation in the BSTI (BSTI, 2023). The quality and performance of the presently used software in the public sector are mostly troublesome because of limited instances where pirated versions of Microsoft products are commonly used. The 'BCS 2021-2025' lacks clear provisions regarding the standardization of software and the use of pirated software in the country.

Cybersecurity is a global phenomenon; it is not bound by international boundaries. It demands effective collaboration and cooperation amongst the stakeholders of government sectors, private sectors, civil society, and international organisations. Most of the KIIs agreed that international collaboration is necessary to develop a resilient cyber environment in the country. BCS 2021-2025 lacks in this regard. Tarique M Barkatullah of the 'Digital Security Agency' has stated that the cybersecurity strategy might make Bangladesh confident, capable, and resilient in this fast-moving digital world. But the reflection of the statement is not entirely complimented in the strategy.

Global Standard and Best Practices of Cybersecurity Strategy

Global Cybersecurity Environment. The global cybersecurity environment is an intricate landscape shaped by the relentless evolution of technology and the escalating threat landscape. As our world becomes increasingly interconnected, the risk of cyber threats has reached unprecedented levels. Nation-states, criminal organizations, and individual actors continuously exploit vulnerabilities in digital infrastructure, posing significant challenges to the security and privacy of individuals, businesses, and governments worldwide. The need for robust cybersecurity measures is paramount, requiring collaborative efforts between nations, industries,

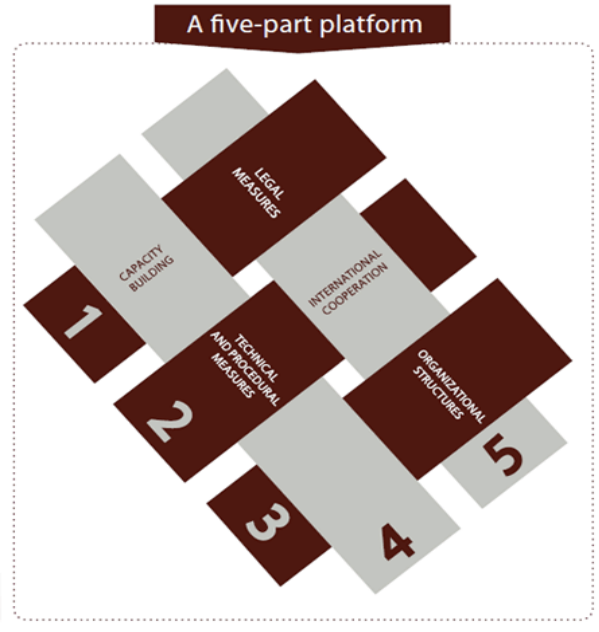
and cybersecurity professionals to develop proactive strategies, share threat intelligence, and implement advanced technologies to safeguard the digital realm from persistent and sophisticated cyber threats.

Global Initiative on Cybersecurity. Over the last decades, ICT's exponential expansion and quick acceptance have benefited billions of people worldwide. Preserving digital assets and ensuring cybersecurity are paramount in today's interconnected world. By embracing internationally recognized standards, a nation can strengthen its defence against cyber-attacks, reduce vulnerabilities, and cultivate a culture of proactive security measures. Cybersecurity has been a top priority on the agenda of the UN (UNGA55/2, 2000). A UN resolution provides a platform for countries to collaborate, share information, and develop common strategies to combat cyber threats (UNGA76/135, 2021). The Budapest Convention on Cybercrime, open for signature in November 2001 in Hungary, is recognized as the foremost international treaty addressing electronic evidence and cybercrime. The Budapest Convention establishes criminal penalties for actions such as the unauthorised use of a computer, tampering with data or systems, and the use of child pornography (COE, 2004).

ITU's Guidance on Cybersecurity Strategy. Though cybersecurity is a global phenomenon, the issue has become a national concern for most countries. The International Telecommunication Union (ITU) is the United Nations specialised agency for ICT. ITU has been established to promote interoperability in communications networks, allot global radio spectrum and satellite orbits, create technical standards to ensure seamless interoperability of networks and technologies and work to increase access to ICTs for underserved global communities. (ITU, 2023). The Global Cybersecurity Agenda (GCA) is an initiative led by the ITU. The GCA aims to foster international cooperation and collaboration in addressing cybersecurity challenges (ITU, 2011). To maintain a secure and resilient cyberspace, nation-states must align their strategy with the five key pillars of GCA, i.e., legal measures; technical and procedural measures; organisational structures; capacity building, and international cooperation

(Uddin, 2017). The five key pillars of the cybersecurity strategy formulation of GCA are given in Figure 2.

Figure 2: Pillars of the Global Cybersecurity Agenda



Source: International Telecommunication Union

Contemporary International Standards in Cybersecurity. Before delving into Bangladesh's strategy, it would be beneficial to discuss recent advancements in global cybersecurity preparedness to comprehend the dynamics of contemporary practices. This study analyses the national cybersecurity strategies of India and the United States because India, as Bangladesh's immediate neighbour, shares similar socio-political realities, while the USA boasts top-tier cybersecurity institutions.

Salient Aspects of the USA's Cybersecurity Strategy. The United States of America recognises the critical importance of cybersecurity in today's digital era. It has developed a comprehensive cybersecurity strategy to protect its national interests and ensure the resilience of its cyber infrastructure (NCS_USA, 2023). The Biden administration released the

new national cybersecurity strategy of the USA by replacing the Trump administration's cybersecurity strategy 2018 on 02 March 2023 (Jindal & Soliman, 2023). The new strategy expands on the former, maintaining momentum on many of its priorities while attempting to carry through and develop many strategic initiatives, initially launched by the 'Comprehensive National Cybersecurity Initiative 2008'.

The USA's cybersecurity strategy encompasses various elements to defend against cyber threats, promote innovation, and foster international cooperation. It emphasises the protection of CIIs, sensitive government information, and the privacy of its citizens. The strategy adopts a multi-pronged approach that includes enhancing cyber defences, deterring malicious actors, and responding swiftly and effectively to cyber incidents. The United States also significantly emphasises public-private partnerships, collaborating with industry leaders to share threat intelligence, strengthen cyber defences, and promote adopting best practices. With its cybersecurity strategy, the United States endeavours to create a secure and resilient digital ecosystem that supports economic growth, innovation, and the protection of its citizens and critical infrastructure.

Salient Aspects of the India's Cybersecurity Strategy. The National Cybersecurity Policy 2013 (NCP-2013) of India was published on 02 July 2013 with a vision "to build a secure and resilient cyberspace for citizens, businesses and government" (DSCI, 2013). The NCP-2013 has provided a comprehensive framework for improving CIIs resilience, protecting sensitive data, and promoting a secure cyberspace for all stakeholders. One of the key strengths of the policy was its focus on public-private partnerships, encouraging cooperation between the government, industry, and academia. The NCP-2013 has provided a comprehensive framework for improving CIIs resilience, protecting sensitive data, and promoting a secure cyberspace for all stakeholders. The Indian government, under the supervision of the 'National Security Council Secretariat' through a task force, is in the process of formulating the National Cybersecurity Strategy 2020 (NCS-2020) for five years (Mallick, 2020). National cybersecurity coordinator Lt Gen (Dr) Rajesh Pant said at a cybersecurity conference that India's NCS-2020 is ready and awaiting cabinet approval.

The vision of the proposed NCS-2020 is "to ensure a safe, secure, trusted, resilient and vibrant cyberspace for the nation's prosperity" (DSCI, 2020). The NCS-2020 aims to secure the "national cyberspace" (presumably Indian interests in cyberspace) by strengthening three pillars of the strategy, secure (national cyberspace); strengthen (structures, people, processes, capabilities) and synergies (resources including cooperation and collaboration), (DSCI, 2020). One of the notable strengths of the strategy is its emphasis on proactive defence and threat intelligence sharing. All organisations must allocate a dedicated budget to implement a cybersecurity strategy. It also fosters collaboration between the government, private sector, and international partners to exchange information on emerging threats and vulnerabilities. R&D will be urged to develop affordable domestic security technologies that will be offered to overseas markets and will address a wide range of cybersecurity concerns.

Critical Analysis of Bangladesh Cybersecurity Strategy 2021-2025

Conceptual Understanding and Analysis Techniques. International Telecommunication Union (ITU) published 'National Cybersecurity Strategy Guide' in 2011 to define a reference model for countries elaborating new or improving existing national strategies on cybersecurity. BCS 2021-2025 is analysed based on cybersecurity strategy development pillars of ITU, i.e., Legal Measures, Technical & Procedural Measures, Organizational Structures, Capacity Building and International Cooperation (GCA, 2007). Finally, the BCS 2021-2025 compares with international standards and best practices of different developed countries.

General Analysis of Bangladesh Cybersecurity Strategy

Insufficiently Defined Vision and Goals. Developing an effective strategy requires meeting several essential conditions. Colonel Arthur F. Lykke Jr. also provided this formula: "Strategy equals ends (objectives toward which

one strives) plus ways (courses of action) plus means (instruments by which some end can be achieved)" (Lykke, 1989). A fundamental requirement of national strategy development is a clear understanding of long-term vision and goals, which defines the desired outcomes and purpose with a deliberate action plan. The BCS 2021-2025 lacks a precise vision, distinct goals, and a time-bound action plan. Dr Mohammad Shafiul Alam Khan has also expressed in an interview, "We have not yet been able to set a long-term vision. Where do we want to see our cybersecurity preparedness after ten years? We must decide urgently (Uddin, 2017)."

Structural Weaknesses. GCA of ITU has suggested the formulation of a cybersecurity strategy grounded in five pillars. However, BCS 2021-2025 has been developed based on the four pillars i.e., digital government, human resource and development, IT industry promotions, and connecting citizens. Since the strategy did not adhere to the GCA's suggested format or the global best practices, several core components of developing cybersecurity strategy remain absent or loosely connected at the BCS 2021-2025.

Inadequate Budgetary Implication and Implementation Plan. A dedicated budget is essential for the effective implementation of the strategy. Both the United States and India have considered the financial ramifications of their cybersecurity strategies (Curran, 2023). The strategy was officially released in January 2022, spanning five years from 2021 to 2025. Until now, most of the stakeholders are not very much aware of their actions and responsibilities. It also lacks in defining the priorities, resources, and time-bounded implementation plan.

Critical Analysis: Legal Measures of BCS 2021-2022

Lack of Comprehensive Cyber Legislation. The cybersecurity strategy of Bangladesh aims to align the country's legal response system against cybercrime with the 'ITU Toolkit for Cybercrime Legislation'. Moreover, it was recommended that the text of the national cybercrime law should comply with the 'Budapest Convention on Cybercrime 2001'. Bangladesh

has yet to ratify it. Most of the KIIs stated that there are concerns about potential infringements on freedom of expression, privacy rights, and global applicability. Hence, the existing cyber legislation of Bangladesh has room for improvement to develop a comprehensive cyber legislation.

Lack of Effective Enforcement of Cyber Law. GoB has enacted the 'Digital Security Act 2018' to strengthen cybercrime enforcement capacity and counter advanced cyber threats. In practice, the law is not being enforced appropriately due to the limited knowledge and expertise of law enforcement agencies and the judiciary in ICT.

Critical Analysis: Technical and Procedural Measures of BCS 2021-2022

Weak Emergency Response System. National Computer Incidence Response Team (N-CIRT), is an essential pillar of global cybersecurity. Therefore, every state needs an N-CIRT to safeguard its critical infrastructure. BGD e-GOV CIRT is presently acting as an N-CIRT for Bangladesh. This small team was formed to provide preventative services like security assessment and intrusion detection. BGD e-GOV CIRT is primarily reactive and provides service to public organisations only. Therefore, private stakeholders remain vulnerable throughout. However, BCS 2021-2025 does not address the requirement of strong BGD e-GOV CIRT to have a 24/7 proactive service delivery capacity.

Lack of Anti-piracy Software Directives. In a recent global software survey by the 'Business Software Alliance', it was disclosed that 37% of software worldwide is unlicensed. Bangladesh holds the highest piracy rate 92% in the Asia-Pacific region (Rahman & Sultana, 2015). This leaves individuals and businesses vulnerable to data breaches, financial losses, and compromised privacy. Hasib M. Rashid, an independent cybersecurity analyst stated that most of the government websites in Bangladesh have outdated security protocols (Mahmud, 2023). The majority of the KIIs have concurred that the BCS 2021-2025 fails to cover the preventive measures for anti-piracy software within the country.

Critical Analysis: Organisational Structures of BCS 2021-2022

Absence of the Focal Point Organisation. The organisational structure of cybersecurity in Bangladesh involves multiple agencies and institutions working together to defend the country's cyberspace and CIs from cyber threats. In the era of 21st century, ICT is spreading at an unprecedented rate. Presently, the ICT Division of MoPT is the apex cybersecurity organization in Bangladesh. MoPT comprises the 'Post and Telecommunication Division' and 'ICT Division'. It faces difficulty in performing as a dedicated focal point organisation for cyber and ICT.

Critical Analysis: Capacity Building of BCS 2021-2022

Inadequate Research and Development (R&D) Policy. Certainly, the enhancement of cybersecurity in any nation undeniably relies on the effectiveness of its R&D efforts. Many developed nations have successfully set up a national cybersecurity research center, acting as a center for excellence in the development of domestic cybersecurity systems. Yet, the aspects of R&D in BCS 2021-2025 are not conceptualized unambiguously. Dr Mohammad Shahriar Rahman mentioned, "The tendency to hire external experts to set up our security systems should be changed. We need a national center of excellence where all cybersecurity expertise will be combined" (Uddin, 2017).

Critical Analysis: International Cooperation of BCS 2021-2022

Absence of International Cooperation and Collaboration. There is no alternative to promoting cooperation at both regional and international levels to ensure the cybersecurity of Bangladesh (Islam, 2021). Most of the interviewees opined that the boundary of cyberspace is not bound by the international border. Therefore, a country or government alone cannot establish a resilient cyber environment in the country. Again, Bangladesh has yet to ratify the 'Budapest Convention on Cybercrime 2001', which is applicable and interoperable worldwide. BCS 2021-2025 lacks to provide

clear directives on international cooperation and collaboration aspects of cybersecurity.

Recommendations

Bangladesh has made commendable strides in achieving a resilient cyber environment within the country by formulating a cybersecurity strategy. Despite the government's admirable efforts, there is room for improvement in various areas, such as the legal framework, organizational structure, public-private partnerships, incident response, and international cooperation. However, the following recommended issues may be addressed while preparing a new cybersecurity strategy for Bangladesh to attain resilient cyberspace in the country:

- While crafting a national cybersecurity strategy, Bangladesh may adhere to the standard structure outlined by ITU, incorporating specific vision, goals, and a time-bound action plan.
- The ICT Division of MoPT could transform into an autonomous ICT Ministry of the Peoples Republic of Bangladesh, serving as the focal point organization for upholding a resilient cyber environment in the country.
- Bangladesh may develop a 'Cybersecurity Master Plan' and formulate a five-year cybersecurity strategy in sync with the five-year perspective plan.
- Bangladesh needs to revisit its legal framework and enact comprehensive cyber legislation aligning with the ITU's recommendations and respecting the fundamental rights of its citizens.
- Bangladesh must enhance its international collaboration and cooperation effort and join different international standard-setting bodies to represent its voice regarding security and privacy.

- Bangladesh may establish a national cybersecurity research center for R&D purposes that can serve as a center of excellence in the development of domestic cybersecurity systems.

Conclusion

The cybersecurity environment of Bangladesh has witnessed significant advancement as well as challenges. The nation has made admirable efforts to fortify its digital infrastructure and safeguard its people, businesses, and government organisations from cyber threats. Enacting acts, policies, and awareness initiatives shows the government's dedication to cybersecurity. However, the government's efforts to secure cyberspace require more evaluation and in-depth investigation. However, the changes suggested in this paper are by no means unrealistic. They are most definitely broadly applicable in the Bangladeshi socio-political situation. Implementation of the recommended policy action may prevent another significant catastrophe like the Bangladesh Bank heist in the upcoming days. Still, a critical analysis suggests the importance of refining certain aspects to maximise its impact and effectively protect the country's digital ecosystem.

References

1. 8FYP, 2020. 8th Five Year Plan July 2020 - June 2025, Dhaka: Economic Division, Ministry of Planning.
2. BCC, 2023. Bangladesh Computer Council. [Online] Available at: https://bcc.portal.gov.bd/ [Accessed 12 April 2023].
3. BCS2021-2025, 2023. Bangladesh Cybersecurity Strategy 2021-2025, Dhaka: ICT Division of MoPT.
4. BSTI, 2023. Bangladesh Standards Testing Institute (BSTI). [Online] Available at: http://www.bsti.gov.bd/ [Accessed 01 May 2023].

5. BTRC, 2023. Bangladesh Telecommunication Regulatory Commission (BTRC). [Online] Available at: http://old.btrc.gov.bd/history-and-vision [Accessed 30 April 2023].

6. CIRT, B. e.-G., 2023. Bangladesh Cyber Threat Land Scape Year 2022, Dhaka: BGD e-GOV CIRT, Bangladesh Computer Council.

7. COE, 2004. Council of Europe. [Online] Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 [Accessed 15 July 2023].

8. DSCI, 2013. Data Security Council of India, New Delhi: A NASSCOM® Initiative.

9. DSCI, 2020. Data Security Council of India, New Delhi: A NASSCOM® Initiative.

10. GCA, 2007. International Telecommunication Union. [Online] Available at: https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx [Accessed 21 June 2023].

11. ICT_Division, 2023. ICT Division of MoPT. [Online] Available at: https://ictd.gov.bd/ [Accessed 10 July 2023].

12. Islam, M. S., 2021. Cybersecurity: A National Piority for Bangladesh. 1st Ed. ed. New York: Routledge Companion to Global Cyber-Security Strategy.

13. Islam, M. S., 2021. Cybersecurity: A national priority for Bangladesh. In Routledge Companion to Global Cyber-Security Strategy. 1st Ed. ed. New York: Taykor and Francis.

14. ITU, 2011. ITU National Cybersecurity Strategy Guide, New York: International Telecommunication Union.

15. ITU, 2023. International Telecommunication Union. [Online] Available at: https://www.itu.int/en/Pages/default.aspx [Accessed 10 February 2023].

16. Jasim, M. M., 2022. The Business Standard. [Online] Available at: https://www.tbsnews.net/bangladesh/bangladesh-final-stages-clearing-cyber-security-strategy-376933 [Accessed 10 April 2023].

17. Jindal, D. & Soliman, M., 2023. The 2023 National Cybersecurity Strategy: How Does America Think About Cyberspace?. Midle East Institute (MEI), p. 01.

18. Kepios, 2023. DATAREPORTAL. [Online] Available at: https://datareportal.com/reports/digital-2023-bangladesh[Accessed 30 April 2023].

19. Lykke, C. A. F., 1989. Defining Military Strategy: S= E+ W+ M. Military Review, Issue May 1989, pp. Page-2.

20. Mahmud, F., 2023. Nikkei Asia. [Online] Available at: Nikkei Asia [Accessed 21 July 2023].

21. Mallick, M. G. P., 2020. India's National Cybersecurity Strategy: How to Go About It. Centre for Land Warfare Studies, Volume 222, p. 01.

22. MoPT, 2023. Ministry of Posts, Telecommunications & Information Technology. [Online] Available at: https://ictd.gov.bd/ [Accessed 10 July 2023].

23. Nation, T., 2011. The Nation. [Online] Available at: https://www.nation.com.pk/11-Dec-2011/developing-states-vulnerable-to-cyber-attacks-says-un [Accessed 10 April 2023].

24. NCS_USA, 2023. National Cybersecurity Strategy, New York: White House.

25. NCS, 2014. National Cybersecurity Strategy 2014, Dhaka: ICT Division of MoPT.

26. Rahman, M. A. & Sultana, S., 2015. Software Piracy in Bangladesh: the Student Perceptions Study on Two Selected Public Universities in Dhaka City. Manarat International University Studies, Issue 4(I), p. Pg 148.

27. Singer, R. & Friedman, A., 2014. Cyber Security and Cyber War What Everyone Needs to Know. 1st Ed. ed. New York: Oxford University Press.

28. Standard, T. B., 2023. The Bussiness Standard. [Online] Available at: https://www.tbsnews.net/bangladesh/agency-innovate-a2i-bill-passed-parliament-660766 [Accessed 31 July 2023].

29. Uddin, M. R., 2017. The National Cyber Security Strategy of Bangladesh: A Critical Analysis. Journal of International Affairs, Volume 1, p. 21.

30. UNGA55/2, 2000. Resolution on United Nations Millennium Declaration, New York: United Nation General Assembly.

31. UNGA76/135, 2021. Resolution on Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, New York: United Nation Geneal Assembly.

32. Whiting, A. & Wiiliams, D., 2013. Why People Use Social Media: A Uses and Gratifications Approach. Qualitative Market Research International Journal, 16(4), pp. 362-369.

Author

Brigadier General Raisul Islam, SPP, ndc, afwc, psc was commissioned in the Regiment of Artillery in 1997. Over his distinguished career, he held various significant appointments in Artillery Regiments. He served as a General Staff Officer at different grades and Brigade Major in an Artillery Brigade. Brigadier General Raisul also contributed to military intelligence as a General Staff Officer Grade II at the Army Headquarters and Directorate General of Forces Intelligence (DGFI) in different capacities. His international experience includes serving in UNMIL as a Platoon Commander and G-1 Chief in MINUSMA. He has commanded both an Artillery Regiment and an Artillery Brigade, showcasing leadership acumen. Additionally, he played a pivotal role in establishing the Army IT Support Organisation. Brigadier General Raisul holds Master Degrees in Military Studies and Business Administration, demonstrating his commitment to both professional and academic excellence. He is a graduate of National Defence College and Defence Services Command & Staff College. He continues to contribute significantly to the defence and security landscape of Bangladesh.

NDC JOURNAL
Security Through Knowledge

THE EMERGENCE OF A FLUID MULTIPOLARITY: CHALLENGES AND OPPORTUNITIES FOR BANGLADESH NATIONAL SECURITY

Air Commodore Md. Zahir Uddin, GUP, ndc, acsc, psc, GD(P)

Introduction

Bangladesh is a rapidly growing economy that holds an important geopolitical position. Despite potentially getting involved with major powers like the USA, China, Russia, and India, Bangladesh has chosen to remain non-aligned. Instead, it focuses on income growth, human development, and reducing vulnerability. The country faces various security challenges due to its strategic location, and it must protect its progress. By staying non- aligned, Bangladesh can maintain good relations with global and regional powers while safeguarding its own interests. This diplomatic strategy is crucial for sustaining economic growth and addressing security challenges such as regional conflicts, terrorism, transnational crime, and climate-related issues.

The global power dynamics are changing as the United States' dominance is shifting, possibly leading to a bipolar or multipolar world order. China's growing influence and Russia's involvement in the Ukraine conflict are contributing to this shift. Other countries such as Turkey, Iran, Qatar, the UAE, Saudi Arabia, Japan, and India also have important roles to play. Bangladesh as a developing nation needs to consider the implications of this changing global landscape. A study will analyze the current geopolitical situation, identify the key players, and evaluate their connections to Bangladesh. Based on the findings, recommendations will be provided to help Bangladesh adapt its foreign policy to navigate this evolving geopolitical environment.

The complex situation in Bangladesh involves significant interest from major players such as the USA, China, Russia, and India. Religious ties with Saudi Arabia, Turkey's Islamic majority, and economic dependencies further complicate the nation's stance. Bangladesh's traditional motto of 'Friendship to all; malice towards none' is challenged by global and regional demands for a clearer position. Amid global financial challenges, the Ukraine conflict, the Rohingya crisis, and escalating US-China tensions, Bangladesh must carefully weigh factors to secure its national interests. This study aims to analyse the fluid multipolarity and its implications, assess ongoing dynamics, and provide policy guidelines for Bangladesh's national security.

The study on "The Emergence of a Fluid Multipolarity: Challenges and Opportunities for Bangladesh National Security" holds significance in understanding shifting global power dynamics. The concept of a fluid multipolarity suggests a departure from a unipolar or bipolar structure, necessitating a deeper understanding for Bangladesh to navigate potential challenges. By identifying challenges and opportunities, Bangladesh can better prepare for the evolving international landscape, strengthen its position, and inform policy decisions related to national security and foreign relations.

Objective and Scope of the Study

The study aims at (i) Gaining foresight into the multipolarity in geopolitics, (ii) Assessing the current geopolitics both regional and international, (iii) Ascertaining the challenges and opportunities, Bangladesh will face in the context of fluid multipolarity, and (iv) Providing foreign policy recommendations for Bangladesh to navigate adeptly the new reality ensuring the nation's sustained development. In pursuit of the study objectives the study aims at exploring answers to following study questions: (a) What is the current geopolitical situation and its impact on Bangladesh? (b) What is the likelihood of a fluid multipolarity in world geopolitics, and which nations are anticipated to be significant players for

Bangladesh? (c) How would potential multipolarity affect Bangladesh? (d) What foreign policy guidelines are crucial for Bangladesh to ensure its ongoing development?

It is not clear under the dynamic nature of the 'Fluid Multipolar' geopolitical scenario, how it will evolve in future and how the world orders will play out. To emphasize more on Bangladesh within the scope of the study, the limitations include the dynamic nature of the fluid multipolar scenario, making predictions challenging. The assumption that China and Russia will contend for world hegemony, the US and EU will remain major world powers, and regional powers will retain their roles guides the study. Due to the vastness of the subject and time constrains, the study emphases on the economic security aspect which is crucial for Bangladesh's development. Further study is required to investigate the rise of new world order and existence of the present international organizations.

Review of Literatures

A comprehensive review of study articles, books, and publications on Bangladesh's Foreign Policy, Economic Development, recent geopolitical developments, and the multipolar world order reveals key insights. The examined literature emphasizes the global shift from a unipolar to a multipolar order, necessitating a redefinition of international norms. Theoretical models offer analytical tools for understanding the current unipolar world order and predicting outcomes, especially regarding state behaviour and small states' challenges.

Small states, including those in NATO, grapple with security challenges such as drones, hybrid warfare, and Russian aggression. Eastern Eurasia is projected to be the new international decision-making theatre, ushering in a period of multipolarity. Bangladesh, in navigating this landscape, faces the intricate task of balancing relationships with major powers like China and India. Strategically hedging its position, Bangladesh leverages its geographic location for geopolitical favour.

The Bay of Bengal emerges as a contested zone, posing security and development challenges for Bangladesh. The relationship between Bangladesh and India, despite shared attributes, remains tense, demanding a reconciliatory approach. In a multipolar world, foreign policy is pivotal for Bangladesh's economic growth and prosperity, requiring adaptability. Bangladesh's security framework demands an adaptive approach integrating national development with multilateral diplomacy, prioritizing regional cooperation. The nation's pragmatic and independent foreign policy aligns it as a significant voice in international affairs, contributing to a more equitable world order.

However, the literature warns that a return to multipolarity, accompanied by great power rivalry, could lead to a less stable world, especially considering the presence of nuclear weapons. In summary, the international structure is shifting towards multipolarity, posing challenges for small states, including Bangladesh, which must strategically navigate geopolitical dynamics and prioritize cooperation for sustainable development.

Methodology

In this study, a qualitative research method is used to gain a thorough understanding of the topic. A descriptive study design is also included to provide a comprehensive overview of the fluid multipolar world order and how it impacts Bangladesh. The literature review analyzes various academic articles, books, reports, and other relevant sources.

During the data collection phase, primary data is collected through interviews with experts, policymakers, and stakeholders in international relations. Surveys and focus group discussions are also utilized. Two case studies are conducted on Singapore's foreign policy and South Korea's foreign policy, focusing on their strategies for economic development and global relations. The collected data is analyzed using qualitative analysis techniques to identify emerging themes and draw meaningful conclusions. This approach allows for a thorough examination of how the changing

multipolar world order impacts Bangladesh, using various qualitative study techniques and data sources.

World Geopolitical Situation, Transformation of World Order, and the Key Players in the Emerging World Order

The global geopolitical landscape has undergone substantial transformations, transitioning from the Cold War's bipolarity to unipolarity with the United States as the sole superpower, and more recently, to a complex multipolarity following the 2008 Global Financial Crisis. The current trend indicates the emergence of multipolarity, driven by factors such as the rise of new economic powers, the global spread of democracy and human rights, and the growing influence of non-state actors.

Transformation of World Polarity

The world, once dominated by the unipolar strength of the United States post-Soviet era, is undergoing a shift towards multipolarity. This shift results from various factors such as political, economic, and social changes. The interconnected nature of the global economy, the rise of transnational issues like climate change and terrorism, and the emergence of new forms of governance through international organizations contribute to this transformative process. Navigating strategic partnerships and understanding complex geopolitical relationships are becoming essential for success in this evolving international environment.

Figure 1: Major World Power States in the Fluid Multipolar World Order

Major World Powers in a Multipolar World

The emerging multipolarity is characterized by major players such as the United States (US), China, Russia, the European Union (EU), India, and Japan. Each of these nations plays a crucial role in shaping the geopolitical landscape, and their present standing, transformations, and prospects are examined.

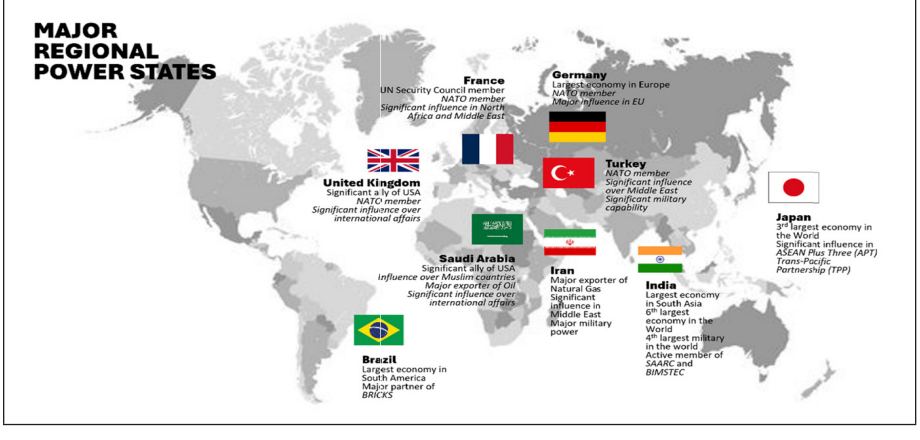
The United States. The US has long been seen as a powerful superpower, but it is now facing challenges to its status because of changes in the global economy, the emergence of authoritarian leaders, and shifts in foreign policy. However, the US still holds significant influence globally, using its military strength, diplomatic connections, and cultural impact. The Trump Administration (as of January 2025) has initiated significant shifts in US foreign policy, signalling a departure from traditional alliances and a reassertion of American dominance on the global stage.

China. China's impressive economic growth, with an average annual rate of 6~7%, has elevated its status as a potential superpower. The Belt and Road Initiative (BRI) further amplifies China's economic influence worldwide. Nonetheless, managing challenges such as international tensions, domestic instability, and human rights issues is crucial to maintain long-term influence.

Russia. Russia, with its vast territory, significant resources, and powerful military, asserts itself on the global stage. Its military capabilities and energy resources contribute to its influence, despite facing economic challenges and growing isolation due to military interventions and alleged interference in other countries' affairs.

European Union. The EU, a powerful economic and political bloc, plays a key role in shaping global politics. Internal challenges such as Brexit and rising nationalism, coupled with external challenges like the rise of China and shifting transatlantic dynamics, require coordinated action for the EU to maintain its significant role in geopolitics.

Figure 2: Major Regional Powers in the Multipolar World Order



Major Regional Powers in a Multipolar World

The increasing influence of regional powers, fuelled by factors such as economic growth, strategic location, resources, political stability, and military strength, complicates the existing world order. Countries like India, Iran, Saudi Arabia, Turkey, Brazil, Japan, and major European nations are becoming important players in their respective regions, shaping global geopolitics. This shift towards a multipolar world presents both challenges and opportunities for nations, necessitating adaptation and collaboration to navigate the complex geopolitical landscape effectively.

National Security and Economic Relations of Bangladesh

Bangladesh has made remarkable progress in poverty reduction and economic growth, with the poverty rate dropping from 44.2% in 1991 to 14.8% in 2016-17. However, as the country experiences rapid economic growth, it faces security challenges related to energy, transport, and urbanization. Situated near India, Myanmar, and China, Bangladesh must address both traditional and non-traditional security concerns to ensure sustained progress.

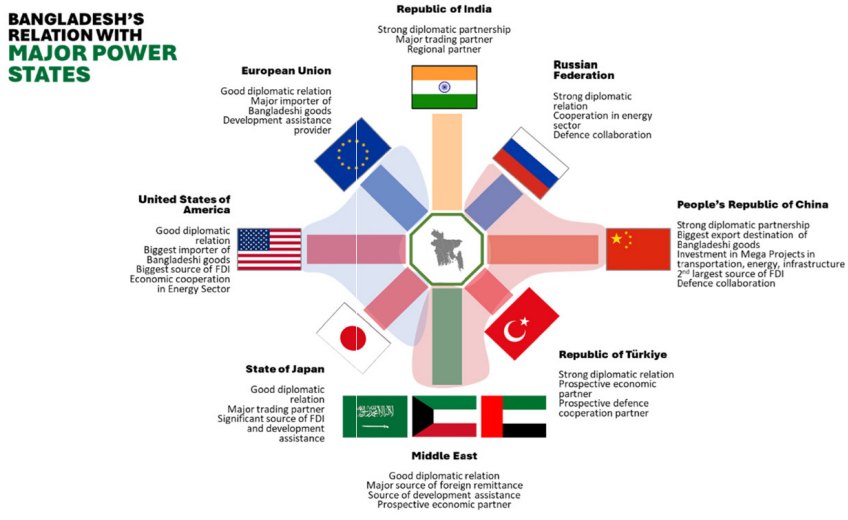
National Security Issues

Bangladesh faces traditional security concerns, including military and non-military threats. Geopolitically, in addition potential military conflicts and unresolved issues pose challenges. The Rohingya crisis remains a significant security concern, with potential implications for regional stability. Transnational threats such as terrorism, arms and drug trafficking, and cybercrime add complexity to the security landscape.

Traditional Security Issues. The close proximity of India and Myanmar creates military risks, and the ongoing Rohingya crisis is a major worry. Political instability, population growth, and poverty worsen security issues. Tensions in South Asia, such as the Pulwama incident and Sino-Indian military stand-offs, contribute to regional conflicts that affect Bangladesh's security. It is crucial for the country's stability to effectively address and handle these problems.

Transnational Security Issues. Bangladesh faces transnational security threats, including terrorism, arms, drug smuggling, human trafficking, climate security, and cybercrime. Although, law enforcement efforts have controlled militant activities, Bangladesh remains vulnerable. Addressing these challenges is vital to safeguard the economy and promote regional stability.

Figure 3: Bangladesh's Relation with Major Power States (Qualitative Assessment)



Economic Relations of Bangladesh

Bangladesh maintains robust economic relations globally, with a focus on diversification. As one of the world's largest garment exporters, the country engages in trade partnerships, attracting foreign direct investment. Economic ties with major players like the US, China, and the EU contribute significantly to Bangladesh's economic growth and development.

Multilateral and Bilateral Economic Cooperation. Developing economic relations with major global and regional powers is extremely important for Bangladesh's development. These relationships provide opportunities for trade, investment, technology transfer, and knowledge exchange. Additionally, they contribute to employment creation, infrastructure development, market access, and regional integration. Bangladesh greatly benefits from its economic ties with countries such as the US, EU, India, and other important nations, which significantly contribute to its economic growth.

Export-Import Scenario. Bangladesh has seen significant growth in its exports, which has helped boost its economy. The main exports are clothing, textiles, jute goods, medicines, and agricultural products. The US, EU, India, and Japan are important markets for these exports. However, the country faces trade deficits due to high spending on imports, particularly machinery, petroleum products, and other necessary items. Balancing domestic demand and reducing dependency on imports is a challenge that requires effective policies.

Characterising Bangladesh's National Security Issues under DIME Model

In analysing Bangladesh's major national issues using the DIME (Diplomacy, Information, Military, and Economy) model, several challenges and strengths come to light:

Diplomacy. Challenges include the Rohingya crisis, with Bangladesh actively seeking international support. Climate change poses a diplomatic challenge, requiring engagement for climate finance and global cooperation.

Information. Challenges involve combating fake news and misinformation spread through social media platforms. Cyber security threats necessitate strengthening national capabilities and fostering international cooperation.

Military. Key challenges include effective border management to prevent illegal activities and recent concerns related to the Kuki-Chin National Front. Counterterrorism efforts require enhanced capabilities, intelligence sharing, and international cooperation. Bangladesh military is dependent on procurement of hardware making it unable to acquire hardware without budget allocation. Therefore, access to military technology through Transfer of Technology or collaboration or joint venture is crucial.

Economy. Challenges encompass poverty and income inequality, demanding focused measures and inclusive economic policies. Infrastructure development requires substantial investments, attracting foreign direct investment and promoting public-private partnerships.

In light of the challenges faced within the DIME model, Bangladesh has the potential to create effective strategies that can contribute to the country's overall development. The following discussion will explore the involvement of major global and regional powers in addressing these domestic issues and safeguarding Bangladesh's national interests.

Geopolitical Influence on Bangladesh by World and Regional Powers

Influence of the United States

The US has a significant influence on important issues in Bangladesh, including diplomacy, information, military, and economy. In terms of diplomacy, the US plays a key role in shaping global relations, particularly in addressing the Rohingya crisis and providing humanitarian aid. The US also has a strong presence in the media and technology sectors in Bangladesh, which can be used to combat misinformation and promote responsible digital media use. Militarily, the US engages in defense cooperation and intelligence exchange, supporting the modernization of Bangladesh's Armed Forces and efforts against terrorism. Economically, the US is a major trading partner and source of foreign investment for Bangladesh, and changes in US trade policies can impact the country's export-oriented industries. The US also provides development assistance in various sectors to promote economic development and social progress in Bangladesh.

Influence of the European Union

The EU has a significant impact on national issues in Bangladesh through its economic, diplomatic, and developmental interactions. It actively engages with Bangladesh in diplomacy, particularly in addressing the Rohingya crisis and advocating for sustainable solutions. The EU supports media development projects and sets global standards for digital rights and privacy, offering valuable expertise to Bangladesh. It also provides military training and assistance, enhancing Bangladesh's capabilities in security and

peacekeeping. As one of Bangladesh's largest trading partners, the EU has influence over trade policies and regulations of Bangladesh, affecting the country's export industries. Additionally, the EU contributes to improving market access, trade relations, and development assistance in education, poverty alleviation, and infrastructure development in Bangladesh.

Influence of China

China has a significant influence over Bangladesh in terms of Diplomacy, Information, Military, and Economy. China's Belt and Road Initiative (BRI) has led to investments in Bangladesh's infrastructure and strengthened diplomatic ties. Chinese companies like Huawei and ZTE are important players in Bangladesh's telecommunications sector. China is a major supplier of defense equipment and provides training programs to enhance Bangladesh's military capabilities. China is also one of Bangladesh's largest trading partners and provides development assistance in various sectors.

Influence of Russia

On the other hand, Russia's influence on Bangladesh is not as extensive but it plays a role in defense cooperation, diplomatic exchanges, and limited presence in the media landscape. Russia supplies defense equipment to Bangladesh and could potentially assist in military technology transfer. Russia's prominence in oil and gas production positions it to contribute to Bangladesh's economy.

Influence of India

The relationship between India and Bangladesh is important for both countries, as they can benefit from working together and addressing common issues. India's influence on Bangladesh is significant due to their shared history, geography, and culture. The two countries have frequent high-level meetings and committees to discuss and address common problems. One important issue is the management of rivers that flow through both

countries, which affects Bangladesh's water resources and agriculture. India's technological advancements also impact Bangladesh's digital landscape, improving connectivity and information-sharing. They also engage in defence cooperation, trade relations, and India has made investments in sectors that have positively impacted Bangladesh's economy. India also provides developmental assistance to Bangladesh in various areas.

Influence of Regional Powers

Turkey has a notable influence on Bangladesh in diplomatic relations, particularly in defense, trade, and education. However, its impact on information-related issues is limited. Japan also has a longstanding relationship with Bangladesh, focusing on infrastructure, trade, and investment. Its influence on information and military aspects is minimal, but it contributes significantly to the country's economic development. Middle Eastern countries like Saudi Arabia and the UAE play a crucial role in diplomatic and economic engagements with Bangladesh, particularly in migration, remittances, and defense cooperation. They contribute significantly to the country's economy through remittances and investments.

DIME Perspective

Through the DIME model, while evaluating major nations' roles in safeguarding Bangladesh's national interest several key considerations emerge:

Diplomacy. Key diplomatic factors include involvement of the US on regional security issue and democratic governance in Bangladesh; involvement of the EU on advocating human rights, good governance, and sustainable development; China's influence through infrastructure investments and economic cooperation; Russia's defense cooperation and diplomatic exchanges; India's substantial influence due to historical, geographic, and cultural ties; Japan's engagement centers on infrastructure development, trade, and investment; Turkey's influence in defense and

economic sectors; and contribution of Middle East countries, notably Saudi Arabia and the UAE, through economic ties and migration issues.

Information. The US, EU, and India significantly impact information exchange, media development, and digital connectivity in Bangladesh.

Military. The US, China, and Russia exert substantial military influence, providing training, equipment, and support to enhance Bangladesh's defense capabilities. India and Japan also engage in defense cooperation.

Economy. China, EU, and India play vital roles in Bangladesh's economic growth through investments, trade relations, and development assistance. Middle East countries contribute through remittances and investment.

The importance of these major nations for ensuring Bangladesh's national interest, the US, EU, China, India, and Japan hold significant influence across multiple DIME elements. Russia, Turkey, and the Middle East have more limited influence but contribute to specific areas aligned with Bangladesh's interests. Therefore, a balanced and strategic approach in engaging with these major nations is crucial for safeguarding Bangladesh's national interest effectively.

Analysis of Challenges and Opportunities in Bangladesh's Development

Bangladesh contends with various challenges amidst the emergence of multipolarity in the global order. The nation is susceptible to the adverse impacts of climate change and rising sea levels, while geopolitical tensions in its region pose diplomatic and geopolitical challenges. Economically, Bangladesh faces challenges of increasing foreign currency reserve, tackling inflation and diversifying its export industry. In the military sphere, the country is modernizing its defense capabilities. While the shift to multipolarity brings both risks and benefits, specific challenges include heightened geopolitical rivalries, diplomatic pressure to align with major power blocs, economic uncertainties, complex regional security dynamics, and changes in international development cooperation.

Examining potential opportunities arising from multipolarity, Bangladesh can diversify its diplomatic engagements, leveraging its strategic location to enhance regional stability. Diplomatically, the country can strengthen ties with emerging powers, participate in multilateral forums, and explore new economic partnerships. Economically, the multipolar world order offers avenues for diversifying trade relations, attracting foreign direct investment (FDI), and exploring new export opportunities. In the military realm, Bangladesh can benefit from international cooperation, technology transfer, and joint exercises, contributing to defense modernization. Moreover, the changing global landscape creates opportunities for development cooperation in infrastructure, sustainable energy, agriculture, and human resource development.

Assessment of Aligning with the United States or China

In the current geopolitical landscape, Bangladesh faces a complex scenario in aligning with either the US or China. Taking a clear side in this major power rivalry could strain relations with the opposing country, potentially leading to political isolation and trade disruptions. However, aligning with a major power offers opportunities for economic cooperation, infrastructure development, and regional connectivity initiatives. The risks include strained diplomatic ties, trade repercussions, and potential security tensions. A nuanced approach is essential, balancing Bangladesh's national interests while navigating the complexities of major power dynamics.

Assessment of Maintaining Friendly Relations with Both the US and China

Maintaining friendly relations with both the US and China presents both challenges and opportunities for Bangladesh. Striking a balance may pose diplomatic challenges, and economic pressures could impact stability. However, friendly ties with both major powers provide diplomatic opportunities, economic cooperation, and potential development support.

In military terms, maintaining balanced relations offers opportunities for defense cooperation, technology transfers, and security collaboration. Careful management is required to avoid straining relationships and to maximize the benefits from both major powers.

Strategy for Bangladesh

Bangladesh faces several challenges today in this multipolar world. Some of the major challenges include political instability, corruption, income and economic inequality, declining global demand for its ready-made garments (RMG) exports, a collapse in remittances, rapidly falling foreign exchange reserves to stabilize the volatility of the Bangladeshi taka, concerns with the demand-supply gaps in the energy markets, inflationary tendencies in the domestic economy, global economic uncertainty, rising inflationary pressure, energy shortages, a balance-of-payments deficit, and a revenue shortfall. In order to manage these challenges, Bangladesh needs to carefully navigate through the geopolitics of rising multipolarity, ensuring support from major and regional powers but at the same time not compromising its national interests. To mitigate challenges and capitalize on opportunities of rising multipolarity, Bangladesh can consider following strategies:

Diversifying Diplomatic Relations. Bangladesh should strive to maintain strong relationships with a wide range of countries, including major powers and regional actors, while upholding its non-aligned foreign policy principles. Strengthening ties with emerging powers and regional organizations can help expand diplomatic options.

Economic Resilience. Bangladesh can focus on diversifying its export base, reducing reliance on specific markets, and promoting value-added industries. It should actively engage in regional economic integration initiatives and explore new markets like BRICS (Brazil, Russia, India, China, and South Africa) nations, the ASEAN (Association of Southeast Asian Nations) countries, South America and Africa to mitigate risks associated with changes in the global trade environment.

Enhancing Defense Capabilities. Bangladesh can invest in enhancing its defense capabilities through modernization programs, training, and international cooperation. It could strengthen relations in this sector with countries like Turkey, Germany, France, China, USA, Japan, South Korea and Middle East, thereby, maintain all blocks of nations.

Innovation and Technology. Embracing innovation, technology transfer, and study and development can enhance Bangladesh's economic competitiveness and resilience. Encouraging entrepreneurship, promoting digitalization, and investing in education and skill development can contribute to long-term growth and development.

Strengthening Regional Cooperation. Actively engaging in regional forums, such as SAARC (South Asian Association for Regional Cooperation) and BIMSTEC (the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation), can foster cooperation, enhance regional stability, and open up opportunities for trade and development. It also can join BRICS to maintain availability of option for continued economic support.

It is important to note that the impact of multipolarity can vary over time, and Bangladesh should remain adaptable, proactive, and forward-looking in its approach to navigate the evolving global landscape.

Foreign Policy Stance of Bangladesh

The foreign policy of Bangladesh is based on the principles of respect for national sovereignty and equality, non-interference in the internal affairs of other countries, peaceful settlements of international disputes, and respect for international law on the principles enunciated in the United Nations Charters. The country pursues a moderate foreign policy that places heavy reliance on multinational diplomacy, especially at the United Nations (UN) and World Trade Organization (WTO). Bangladesh's foreign policy stance in regard to the rising multipolarity in world politics needs to be guided by

its long- standing principles of maintaining a non-aligned and independent foreign policy. Bangladesh should seek to maintain friendly relations with all countries and actively engages in regional and international forums to promote its national interests and contribute to global peace and stability. Two case studies were conducted on Singapore and South Korea, from which valuable lessons were gleaned to establish specific directives and guidelines for foreign policy of Bangladesh. Some key elements that Bangladesh should follow in its foreign policy in the geopolitical landscape of rising multipolarity are briefed below:

Non-Alignment. Bangladesh should adhere to a non-aligned foreign policy, aiming to maintain equidistance from major power rivalries and avoid entanglement in geopolitical conflicts. It should maintain good relations with all countries and blocks to promote dialogue, cooperation, and mutual understanding.

Friendship to All, Malice Towards None. Bangladesh must continue to emphasize on friendship, cooperation, and mutual respect in its interactions with other nations. It needs to build strong bilateral relations based on common interests, shared values, and mutual benefit, while avoiding hostility or confrontation.

Regional Integration and Cooperation. Bangladesh actively participates in regional organizations such as SAARC, BIMSTEC, and IORA (Indian Ocean Rim Association). It promotes regional integration, economic cooperation, connectivity, and people-to-people exchanges in South Asia and the broader region. Bangladesh needs to avoid military alliances but at the same time must engage in economic cooperations within and beyond its regional boundaries to create options for continued economic development. Joining BRICS therefore, may be an opportunity for Bangladesh.

Multilateralism. Bangladesh must rely on multilateralism and actively engage in various international forums, including the United Nations (UN), the World Trade Organization (WTO), the Non-Aligned Movement

(NAM) and the Belt and Road Initiative (BRI). It needs to utilise the opportunity to establish itself as an advocate for global cooperation, collective problem-solving, and the principles of international law for developing nations across the globe.

Development Priorities. Bangladesh's foreign policy should be strongly oriented toward achieving its development goals. It has to keep scope open for international cooperation and assistance in areas such as poverty alleviation, infrastructure development, education, healthcare, climate change adaptation, and disaster management.

Humanitarian Diplomacy. Bangladesh must actively engage in humanitarian diplomacy, particularly in addressing global challenges such as the Rohingya refugee crisis. It needs to ensure requisite support from USA, EU, China, Middle East and India is resolving Rohingya Crisis.

Climate Change and Sustainable Development. As a climate-vulnerable nation, Bangladesh ought to place great emphasis on climate change mitigation and adaptation. It should stress for global action on climate change and actively participate in international negotiations and initiatives related to sustainable development.

Overall, Bangladesh's foreign policy stance in the context of rising multipolarity needs to be characterised by the principles of non-alignment, friendship with all nations, regional integration, multilateralism, development priorities, humanitarian diplomacy, and addressing climate change. It must navigate the complex dynamics of the evolving global order to safeguard its national interests, promote peace, and contribute to global stability and development.

Conclusion

Current global landscape is characterised by emergence of new power structures and evolving dynamics between nations and regions. The pre-existing unipolar world order has weakened to a stage where multiple

nations have emerged to contend for hegemony and at the same time, regional powers have risen to prioritise regional goals above hegemonic ambitions. This paradigm shift has resulted in the simultaneous rise of multiple influential actors, such as nations, organizations, and regional blocs, each asserting their influence on global affairs. As alliances form and dissolve, economic interdependencies deepen, and technological advancements reshape communication and warfare, the world order becomes increasingly intricate and adaptable. The analysis of challenges and opportunities arising from the fluid multipolar geopolitical situation has shed light on the intricate landscape that shapes Bangladesh's national interest. Bangladesh must steadfastly navigate the challenges and harness the opportunities presented by this evolving global order. By adopting a pragmatic approach and embracing policy guidelines derived from this analysis, Bangladesh can effectively address the challenges posed by economic, security, diplomatic, and technological factors. Simultaneously, it can seize the opportunities for economic growth, regional cooperation, technological advancement, and diplomatic engagement. With adaptability, strategic decision-making, and a commitment to sustainable development, Bangladesh can chart a course that ensures its ongoing progress and propels it towards to achieve its goals.

References

1. Ahmed (April 2023). Dr. Qazi Kholiquzzaman (Chairman, Dhaka School of Economics and Palli Karma-Sahayak Foundation), Economy and Development: Road to Progress for Bangladesh, Presentation at National Defence College Dhaka on 02 April.

2. Ahmed (January 2023). Dr. Imtiaz (Professor of International Relations and Director, Centre for Genocide Studies, University of Dhaka), The Nation State System, Presentation at National Defence College Dhaka on 22 January.

3. Al Mabrur, S., Bangladesh's Strategic Hedging towards India and China: Challenges and Options.

4. Alam (April 2023). Dr. Shamsul, (State Minister, Ministry of Planning, Bangladesh), Outcome Based Development Performance of Bangladesh and a Journey Forward, Presentation at National Defence College Dhaka on 30 April.

5. American vs. Chinese Systems of Alliances and Accords in the Asia-Pacific Region, Institute of New Europe. [online] Available at: https://ine.org.pl/en/american-vs- chinese-systems-of-alliances-and-accords-in-the-asia-pacific-region-maps.

6. Bangladesh Overview: Development news, research, data | World Bank. Available at https://www.worldbank.org/en/country/bangladesh/overview.

7. Bhowmick, S., 2023. A Troubling Economic Trajectory in Bangladesh, The Diplomat, 13 January 2023.

8. Brady, A.M. and Thorhallsson, B. eds., 2021. Small states and the new security environment. Cham: Springer.

9. China's influence in South-East Asia has grown. America's has waned. [online] Available at: https://www.economist.com/graphic-detail/2023/06/12/chinas-influence-in- south-east-asia-has-grown-americas-has-waned.

10. Chukwuemeka, E.S., 2021. Problems Facing Bangladesh and Solutions. [online] Available at https://bscholarly.com/problems-facing-bangladesh-and-solutions.

11. Dar, A.A., Mishra, R. and Ahanger, G.A., India-Bangladesh Relations During Modi Regime: An Analytical Study. [online] Available at https://www.researchgate.net/publication/366956774.

12. Economic Community of West African States (ECOWAS) - Strategic-Capacities Assessment by Humanitarian Futures Programme by King's College London.

13. Hansen, B., 2010. Unipolarity and world politics: A theory and its implications. Routledge.

14. How China Is Challenging American Dominance in Asia - The New York Times. [online] Available at: https://www.nytimes.com/interactive/2018/03/09/world/asia/china-us- asia-rivalry.html.

15. John Pike Global Security, 2023, Bangladesh – Foreign Relations. [online] Available at: https://www.globalsecurity.org/military/world/bangladesh/forrel.htm.

16. Kassab, H.S., 2022. Globalization, Multipolarity and Great Power Competition. Taylor & Francis Group.

17. Mahmud (April 2023). Dr. Wahiduddin, (Former Advisor to the Caretaker Govt of Bangladesh), World Economic Scene, Presentation at National Defence College Dhaka on 09 April.

18. Mahmud, K.U. and Jabin, N., 2022. Responses of Bangladesh and Myanmar to the Ukraine Crisis: A Comparative Analysis from a Neo-Classical Realist Perspective. [online] Available at https://www.researchgate.net/publication/366848349.

19. Ministry of Foreign Affairs, Government of Peoples Republic of Bangladesh, 2018, Foreign Policy of Bangladesh, [online] Available at: https://mofa.gov.bd/site/page/0498e3d1-9bb7-45f0-988c-cb360e9949e2/Foreign- Policy-of-Bangladesh.

20. Peters, M.A., 2022. The emerging multipolar world order: A preliminary analysis.

21. Educational Philosophy and Theory, pp.1-11.

22. Quibria, M.G., 2019. Bangladesh's Road to Long-term Economic Prosperity: Risks and Challenges. Springer.

23. Rahman, M.S., 2022. Bangladesh Foreign Policy Towards India: Late 20th–Early 21st Century (Economic Aspect). Asian Profile. [online] Available at https://www.researchgate.net/publication/361016596.

24. Rahman, W., 2021, Five Challenges for Bangladesh in 2021, Op Ed, Dhaka Tribune, 23 February 2021.

25. Siddiquee, M.A., 2022. Great Power Rivalry in the Indian Ocean Region and Bangladesh: Challenges and Responses. Journal of Bangladesh and Global Affairs, 1(02).

26. South Korea Seeks to Balance Relations with China and the United States. [online] Available at: https://www.cfr.org/report/south-korea-seeks-balance-relations-china- and-united-state.

27. Tomja, A., 2014. Polarity and International System Consequences. Interdisciplinary Journal of Research and Development, 1(1), pp.57-61. [online] Available at https://www.academia.edu/34155839.

28. Varisco, A.E., 2013. Towards a Multi-Polar International System: Which Prospects for Global Peace?. E-International Relations Students, 3. [online] Available at https://www.e-ir.info/2013/06/03/towards-a-multi-polar-international-system- which-prospects-for-global-peace.

29. Wade, R.H., 2011. Emerging world order? From multipolarity to multilateralism in the G20, the World Bank, and the IMF. Politics & society, 39(3), pp.347-378.

30. Walton, C.D., 2007. Geopolitics and the great powers in the 21st century: multipolarity and the revolution in strategic perspective. Routledge.

31. Zaman (May 2023) Dr. Rashed Uz (Professor of Department of International Relations, University of Dhaka), Regional Cooperation and Development of Bangladesh, Presentation at National Defence College Dhaka on 10 May.

Author

Air Commodore Md. Zahir Uddin, GUP, ndc, acsc, psc, GD(P) is commissioned on 31st May 1994 in Bangladesh Air Force as General Duties (Pilot) branch. He has had a distinguished career, holding various command, staff, and instructional appointments. He has commanded two operational fighter squadrons and served as an Officer commanding of the Cadets' Wing and later Chief Instructor at the BAF Academy. He has also served as Directing Staff at the Defence Services Command and Staff College. Besides, he played a key role in establishing the 'Aviation Operation Management' department at 'Bangabandhu Sheikh Mujibur Rahman Aviation and Aerospace University'. Currently, he is pursuing a Master's degree in Social Science at 'Bangladesh University of Professionals' in the academic year 2022-23.

NDC JOURNAL
Security Through Knowledge

CLIMATE CHANGE AND REGIONAL SECURITY: CHALLENGES FOR WEST AFRICA

Captain Musa Danjuma Jarma, ndc

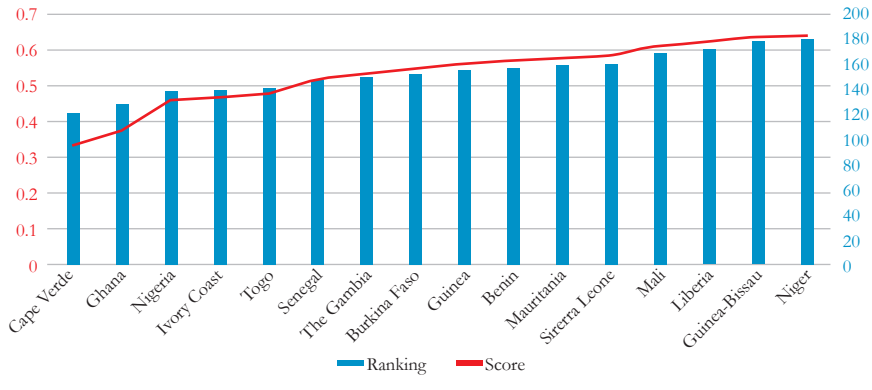
Introduction

Throughout history, people have struggled to acclimate to the environment's many challenges. Of these challenges, the ever-changing adverse climatic condition referred to as climate change has been the most daunting and difficult ever faced by humans (IPCC, 2021). Climate change is taunted as responsible for increasing natural disasters such as floods, droughts, heat waves, and wildfires, which have brought to the fore the consequences of climate change to humanity (FAO, 2021). Consequently, there is now a global political and scientific consensus that the world is suffering from climate change that is adversely impacting livelihoods and the environment. While global efforts are focused on adapting and mitigating the impact of climate change, it is widely accepted that it is practically impossible to avoid some consequences, one of which is its security-related challenges. This is because climate change leads to rivalry and unhealthy competition over limited land spaces and scarce natural resources that have manifested in various forms of security challenges as a threat multiplier, with significant impacts on national and regional security (Seiyefa 2019). Climate change-related security challenges could also exacerbate existing tensions or create new security challenges in a country or region.

Recently, concerns have grown regarding the connection between climate change and regional security in West Africa. This is because most security challenges which were hitherto perceived to arise from local political differences are now taken a wider transnational undertone due to climate change as a multiplier. This is because West Africa is predominantly a subsistence agrarian society that depends mainly on rain-fed agriculture and nomadic livestock rearing, which accounts for 66 percent of the region's

total employment (FAO, 2021). Regrettably, the agricultural sector is the hardest hit by climate change, which has severely impacted livelihoods in the region as attested by the Notre Dame Global Adaptive Initiative Report 2020 (ND-GAIN) as shown in Figure 1. This has increased the population's susceptibility to an array of interwoven climate change-related security challenges such as extremism, violent conflicts, forced displacement of persons, forced migration, unemployment, energy crises and challenges to governance, among others as shown in Figure 1.

Figure 1: West Africa Ranking for Climate Change Vulnerability



Source: ND-GAIN Report 2020.

Pertinently, no region of the world is absolved from the menace of climate change-related security challenges. However, the peculiarity of West Africa's inherent challenges therein, such as vast ungoverned land areas, weak state institutions, political instability, coups, and policy inconsistencies, presents a more severe and challenging dimension to the issue of climate change which shapes the core of the region's security architecture, that must be addressed to enhance regional security. However, there are very few studies on how climate change impacts the current dynamics of security challenges in West Africa and how it could be tackled, which this study is predicated on.

Objectives of the Research. The main objective of the research is to examine climate change's effect on West Africa's regional security. The specific objectives are to assess the prospects of the strategies for reducing the impact of climate change-related security challenges as well as the challenges therein and measures for tackling the challenges.

Research Questions. The primary question is to identify the effects of climate change on regional security in West Africa. The secondary questions include identifying the prospects of the strategies for reducing the impact of climate change-related security challenges, identifying the challenges therein and the measures for tackling the challenges.

Review of Literature

Understanding Climate Change. The word climate change like other widespread social issues, resists a single, inclusive, and generally agreed description but depends on context. While some argue that it is an unnatural occurrence, others argue otherwise. The United States Environmental Protection Agency (USEPA) defined climate change as some anomaly in the climate system caused by the activities of humans (anthropogenic) that increase carbon emissions into the atmosphere causing an increase in greenhouse gases (USEPA, 2023). This argument was supported by the Intergovernmental Panel on Climate Change (IPCC). In its Sixth Assessment Report, it cited that climate change is a change in the state of the climate that can be identified by changes in the mean and the variability of its properties that persists for an extended period, typically decades or longer, whether due to natural variability or because of human activity (IPCC, 2022). USEPA and IPCC 2022 understanding of climate change supports the argument of this research in parts. However, it is pertinent to note that there is yet to be a generally accepted understanding of climate change, especially in the context of regional security because of the multiplexed factors of security. Notwithstanding, the view by USEPA and IPCC has the potential to put to rest the various arguments on climate change in the framework of this study. They may have their relative

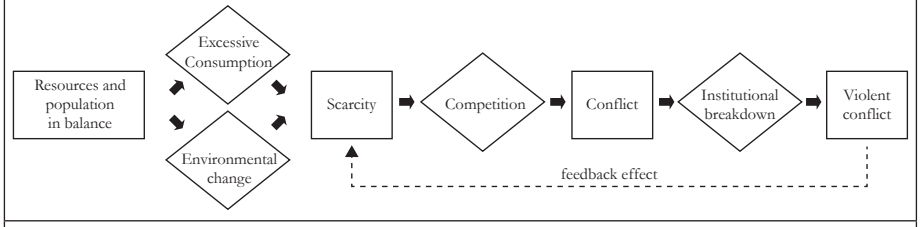
vagueness, but they are concepts that could form the basis for improved regional security for this study.

Understanding the Concept of Regional Security. Regional security has taken on diverse meanings throughout history. In 2003, Barry Buzan and Ole Weaver coined the term 'Regional Security' to describe the nature of conflict between governments in a particular geographic region. According to them, regional security is characterised by the arrangement within security frameworks in each region based on the idea that there are both powerful and weak states in the world, with the region having the weakest states being prone to instability. Within this context, an intermediary concept that filters international security standards, considering regional norms, traditions, and interests, makes up regional security (Buzan et al., 2003). In the present international system, the understanding and practice of regional security are constantly changing, arising from the influence of many military alliances and pacts from the World Wars era, which are directly related to a nation's national security interests and concerns. This changing trend highlights the fluidity of regional security based on shared common security interests and concerns. This invariably means that once the common security interests and concerns seize, the regional security alliance/pact also weans. This is more so that the prevailing security realities in the world transcend international borders and have necessitated the adoption of different types of regional security arrangements in the forms of collective security, self-defence, and deterrence. As a result, new security techniques are rapidly developed, tested, and progressively entrenched into regional security. Invariably, countries that seek to improve their security should choose to be members of broad cooperative regional security networks, which this study is predicated on.

Conceptual Relationship between Climate Change and Regional Security. Studies have indirectly linked climate change and regional security. This is because climate change causes resource scarcity, which leads to unhealthy competition and then results in conflict or accentuates already existing security problems in a region. Brown (2007) postulated the

indirect linkage between climate change and security, as shown in Figure 2. The model indicates that conflict is indirectly linked to resource scarcity caused by environmental changes and excessive resource consumption, which are the outcomes of climate change. The struggle for such scarce resources would lead to higher consumption, and fuel violent conflict. More so, persons displaced by the conflict may create a spill-over effect by demanding resources elsewhere, which may also result in another cycle of conflict (Brown et al., 2007). Such a situation is exacerbated in West Africa by spill-over effects in the vast ungoverned spaces particularly at international border areas.

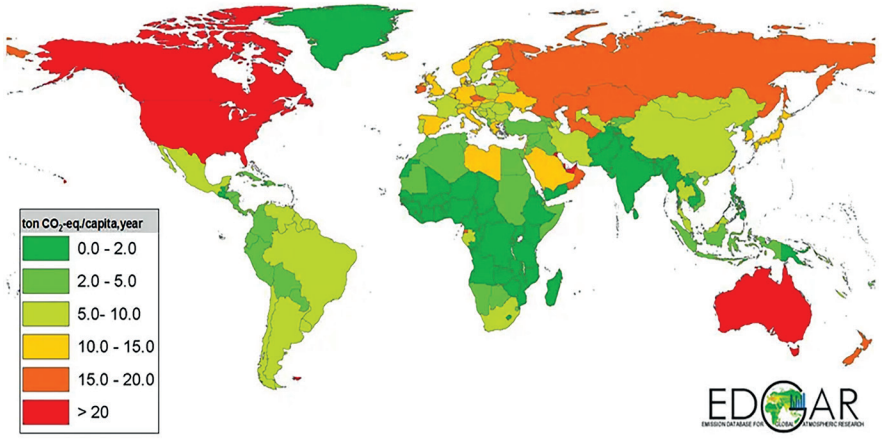
Figure 2: Brown's Model



Source: Adopted from Brown (2007) "Climate Change as the New Security Threat"

Several debates on climate change by the United Nations Security Council (UNSC) beginning in 2007, largely agreed that the changing climate phenomenon poses a considerable danger to international peace and security. Relevantly, the UNSC noted that Africa, which is the least responsible for greenhouse emissions, was the most susceptible to the effect of climate change and its security-related consequences, as shown in Figure 3 (UNCCC, 2018). Subsequent UNSC Climate Change debates in 2011 paved the way for adopting UN Resolution 2349 in 2017 to address climate-induced risks and tackle the security-related challenges in West Africa. This was closely followed by the UN Climate Debate 2018 on understanding and addressing climate change-related security challenges in Africa.

Figure 3: Green House Emission



Source: EDGAR 2022 Climate Report

At the defence level, climate change directly impacts a nation's defence infrastructure and capabilities. Military forces may need to redirect resources to deal with climate-related emergencies, natural disasters, or humanitarian crises. Besides, critical infrastructure, such as energy facilities and transportation networks can be vulnerable to climate change. Damage to these infrastructures can disrupt economies and potentially compromise national and regional security. On the diplomatic scene, where global leaders failed to concur to a binding agreement to curtail climate change, more wars and associated conflicts could ravage climate change-prone areas across all world regions.

Review of Relevant Studies. Studies by Başar Baysal and Uluç Karakas (2017), Seiyefa (2019), Marshall Burke (2019), Blanche Verlie (2022), and Richard Matthew (1995) were identified as the most relevant to this research. From the literature reviewed, the major takeaway is that climate change is currently impacting all facets of livelihoods in the world, West Africa inclusive. This has led to scarcity of natural resources, food shortages and unbearable living conditions that are constantly raising the optics of human survival. Consequently, the studies were in consensus that the intensity of the effects of climate change is fuelling the spate of insecurity around the

world including West Africa. However, the studies had gaps on how local, national, and regional collective approach mechanisms can be harnessed to reduce the effect of climate change-related security challenges especially for a region like West Africa. This is of particular importance because the spill-over effect of security challenges transcends all levels of society in West Africa, which has continued to redefine the security architecture of the region. This is the gap that this research seeks to examine and address.

Theoretical Framework

Homer-Dixon Theory. The Homer-Dixon Theory highlights the relationship between conflict, adaption, population growth, and environmental scarcity. Homer-Dixon argues that the genesis of environmental scarcity caused by climate change weakens the social structure of society and results in conflict (Homer, 1994).

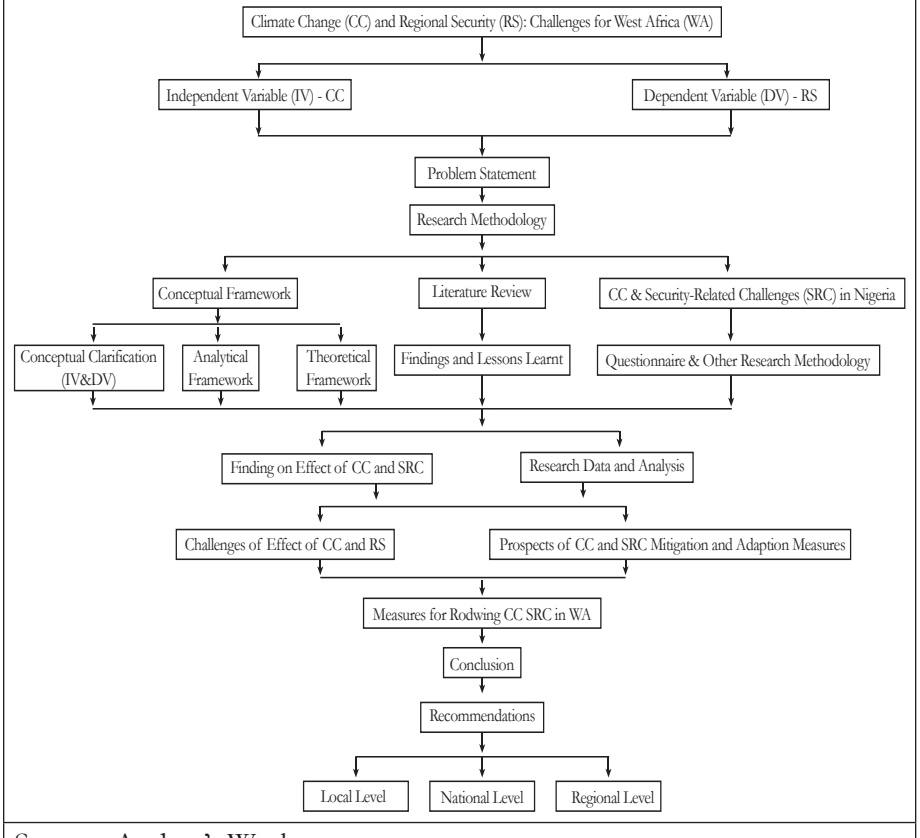
Securitisation Theory. Securitisation Theory postulates, that any concerns or challenges can be translated into security concerns through authoritative, institutional, or political discourse. The Theory illustrates that national security policy does not exist naturally but is formulated by decision-makers (Buzan et al., 1998). Thus, issues are deemed national security challenges when designated as dangerous or threatening by security institutions and appropriate action(s) taken.

Research Methodology

An empirical approach was adopted for this research using quantitative and qualitative data. The research method used in this study is descriptive that examines the interconnectivity between the independent variable (climate change), and the dependent variable (regional security) to draw facts from the problem. Accordingly, the study covered West Africa with Nigeria as a case study from 2017-mid-2023, when there were heightened climate change-related security challenges. Data obtained from the primary sources were 193 respondents' views through questionnaires as well as focus group discussions with 7 subject matter experts based on unstructured interviews. Secondary data sources were unpublished materials, newspapers, seminars,

books, official publications, lectures, policy papers, magazines, journals, conference papers, and the Internet. For analysing the data, the percentage method as well as pie and bar charts were adopted. However, there were some limitations such as the large proportion of the research population to the relatively small number of the randomly sampled population. More so, some people have preconceived ideas about the subject, which could have influenced their responses. Furthermore, some respondents were reluctant to give some information they considered confidential. However, these limitations were not significant enough to negate the research outcome, as the data collected were objectively analysed. To put these into context, the conceptual framework used for the study is shown in Figure 4.

Figure 4: Conceptual Framework



Source: Author's Work

Analysis of Data and Results

Effects of Climate Change on Regional Security in West Africa

The study identified 7 climate change security-related challenges in West Africa as summarized in Table 1.

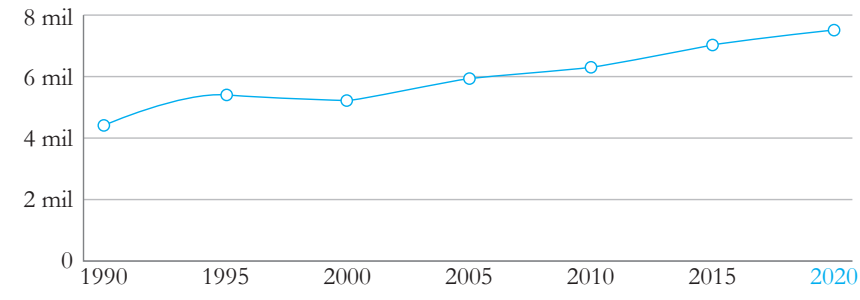
Table 1: Types of Security Challenges Caused by Climate Change

Type of Security	Examples of Main Threats
Economic Security	Persistent poverty, unemployment
Food Security	Hunger, famine
Health Security	Deadly infectious diseases, unsafe food, malnutrition, lack of access to basic health care
Environmental Security	Environmental degradation, resource depletion, natural disasters, pollution
Personal Security	Physical violence, crime, terrorism, domestic violence, child labor
Community Security	Inter-ethnic, religious and other identity based tensions
Political Security	Political repressions, human rights abuses

Source: Human Security Unit of United Nations

Most of these security threats are complex, multifaceted, and interrelated, which makes them daunting and persistent. For instance, climate change directly impacts agriculture and livestock rearing (food security), significantly leading to hunger, malnutrition, and poor health (health security). This, in turn, increases poverty, unemployment, and other socio-economic problems (economic security). Unfortunately, such problems worsen because West Africa comprises of arid and semi-arid desert to the north, which makes it vulnerable to drought, while the southern part is mainly low-lying topography, which makes it vulnerable to flooding (environmental security). This situation forcefully displaces people with attendant security consequences as shown in Figure 5.

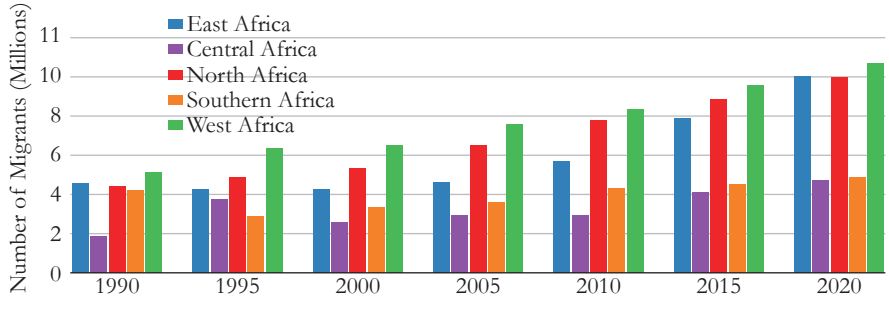
Figure 5: Trend of Internally Displaced Persons in West Africa



Source: UNDECA Report, 2021

Sadly, these displaced persons are helpless and vulnerable to subversion or exploitation into child labour, domestic violence, crimes, and other vices, which have continued to exacerbate insecurity in the region (personal security). The spate of forced displacement has been taunted to exacerbate the rate of transborder migration in the region as shown in Figure 6, which resulted in open confrontations in the form of ethnic, religious, and other identity-based violence and tensions amongst the migrants and host communities (community security). In some cases, the spill-over effects could overstretch and weaken state structures and intuitions, which results in varying perceptions of the action or inaction of governments to the point of diplomatic tension between member states (political security).

Figure 6: Trend of Migration in West Africa



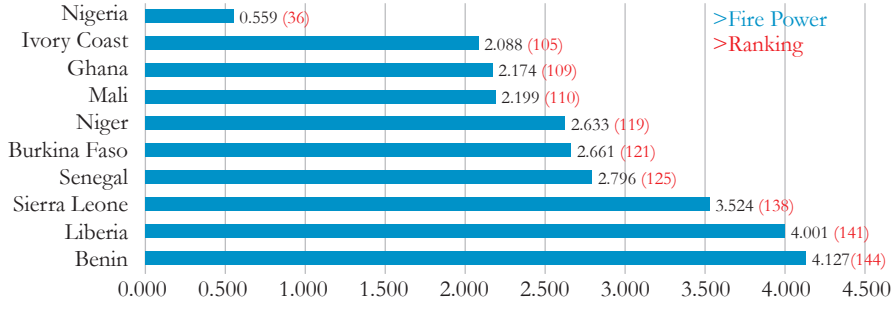
Source: UNDECA Report, 2021

Security Challenges Caused by Climate Change in West Africa

Inadequate Capacity and Capability of Security Mechanisms. The study survey suggests that West Africa lacks the required training and equipment for its security observers and responders to deal effectively and efficiently with security challenges let alone climate-related ones.

One of the major reasons for this challenge is that most of the impacted communities are in harsh and isolated environments with limited/poor infrastructure, which require specialised security equipment and training that are inadequately available for security responders (Jibrin, 2022). This is worsened by the low defence technological base and poor defence industry capability of the region. Hence, West African countries are overreliance on developed nations for the supply of security and defence articles. This comes with many challenges ranging from high equipment costs, bureaucratic procedures, transportation costs and conspiracy associated with foreign defence supplies, amongst others. Thus, it is increasingly difficult for West African states to acquire adequate capability for their security and defence needs, reflecting their dismal ranking on the Global Fire Power Index (GFPI) in Figure 7.

Figure 7: Global Firepower Ranking of West African States



Source: 2023 Global Fire Power Ranking

Poor Framework for Coordinating Stakeholders in Managing Climate Change-Related Security Activities. Mechanisms of addressing climate change-related security challenges in West Africa at the local, national, and regional levels must move beyond reaction and address underlying causative factors. Unfortunately, there is no stand-alone legislative framework for addressing climate change-related security challenges in West Africa. Pertinently, stakeholders at various levels have advanced salient initiatives aimed at tackling climate change-related security challenges but to no avail. While these initiatives are meant to complement each other, most of them are observed to be duplications of efforts, which would have been more effective if well-integrated and coordinated under a common framework. In cases where such a framework exists, it is deficient in providing the requisite guidelines for promoting synergy of effort amongst stakeholders.

Lack of Coordinating Platform for Stakeholders in Managing Climate Change Security-Related Activities. A coordinating platform, which coordinates and directs the management of climate change-related security activities, is critical to local, national, and regional security efforts. In West African states where a coordinating platform exists, concerns often arise about its effectiveness and efficiency, while in other cases, such platforms are highly deficient or do not simply exist. Thus, despite the ratification of international policy frameworks on climate change by West African states such as the 2015 Paris Climate Agreement, there are gaps in its implementation due to poor synergy, coordination, and inadequate working data due to the lack of a coordinating platform. Consequently, the desired policy/strategy direction and action plan become faulty, inconsistent, and ineffective, which mislead decision-making and result in unintended security consequences, hence the need for a coordinating platform.

Poor Governance of Managing Climate Change and Security-Related Activities. West Africa's history is replete with armed conflicts, civil wars and coup d'états that highlight the region's vulnerability to security

challenges despite regional initiatives on peace and security. For instance, the region has witnessed about 150 coups/attempted coups since 1960, with 8 coups/attempted coups between 2020 and to 2022 (Megan et al., 2022). These security concerns tend to spill over by drawing the attention of regional non-state actors, which can significantly complicate the already existing climate change-related security challenges. This unfortunate situation portrays a significant setback for regional-centred initiatives and commitment to climate change policies and strategies in West Africa

Most Conflicts in West Africa are Caused by Natural Resource Struggles. These natural resources are government-controlled, which bring to the fore the importance of resource governance in the region. Resource governance affects critical decision-making in environmental laws, resource control, and extractive industry regulation. Therefore, as climate change alters the availability of these natural resources, especially in transborder areas, it also influences the governments' responses to the resultant struggle, accentuating perceived inequalities and grievances, which may lead to conflict. Also of importance is that, despite global focus on climate change, the matters of climate change in most West African states are often generalised as issues of 'Environment' hence the choice for the designation of the ministries handling such matters as shown in Table 2 except for Burkina Faso and The Gambia. Suffice it to say that the word 'Environment' encompasses several environmental issues with climate change at the heart of the global discussion. Hence, there is an ongoing global awareness consensus of bringing to the fore the word 'Climate Change' to prominence in the nomenclature of concerned authorities to awaken public consciousness on the subject, an idea which is still trivial in West Africa is highlighted below:

Table 2: Ministries Responsible for Climate Change Matters in West African States	
Countries	**Names of Ministries**
Benin	Ministry of the Environment and Sustainable Development
Burkina Faso	Ministry of the Environment, Green Economy, and Climate Change
Cape Verde	Minister of Environment, Rural Development and Marine Resources
The Gambia	Ministry of Environment, Climate Change and Natural Resources
Ghana	Ministry of Environment, Science, Technology, and Innovation
Guinea	Ministry of Environment, Water and Forestry
Guinea-Bissau	Minister of Environment and Biodiversity
Ivory Coast	Ministry of the environment and sustainable development
Liberia	Ministry of agriculture and the Ministry of Land, Mines and Energy
Mali	Ministry of Environment, Sanitation and Sustainable Development
Mauritania	Ministry of Environment and Sustainable Development
Niger	Ministry of Environment
Nigeria	Federal Ministry of Environment
Senegal	Ministry of Environment and Sustainable Development
Sierra Leone	Ministry Of Environment
Togo	Ministry of the Environment, Sustainable Development, and Nature Protection
Source: Author's Field Survey	

Findings

Prospects of the Strategies for Reducing the Effect of Climate Change Security-Related Challenges in West Africa. The strategies for reducing the effect of climate change-related security challenges in West Africa should be a concerted effort at the local, national, and regional levels. These efforts should be aimed at building a climate-resilient society that can resist or recover quickly from the effect of climate change that would rather result in insecurity or reduce the intensity of the insecurity to the barest minimum. Most West African states have made frantic efforts on some of these measures with varying levels of success, however, more needs to be done (IPCC, 2022). The strategies comprise mitigation and adaptation measures. Mitigation measures are geared toward reducing the emission of greenhouse gases, enhancing resilience, and preventing security-related challenges, while adaptation measures combine short and long-term measures that foster resilience and sustainable coping mechanisms. It is essential to note that most of the outlined measures apply to both mitigation and adaptation measures depending on the context. These measures include but are not limited to the renewable and sustainable energy transition, afforestation and reforestation, sustainable agriculture, climate-resilient farming practices, energy efficiency and climate-friendly transport. Others are water management techniques, climate-resilient infrastructure and housing, climate finance, education and awareness, policy and regulation, regional cooperation, early warning systems, community-based adaptation, biodiversity conservation, community policing and protection force.

Measures for Tackling Climate Change-Related Security Challenges in West Africa. Enhancing the Capacity and Capability of Security Mechanism. Enhancing the capacity and capability of security mechanisms could be achieved through a multifaceted approach centred on providing modern training, equipment and advanced technology tailored towards the region's environment. At the local level, training on community outreach programs can be inculcated to train security personnel in comprehending

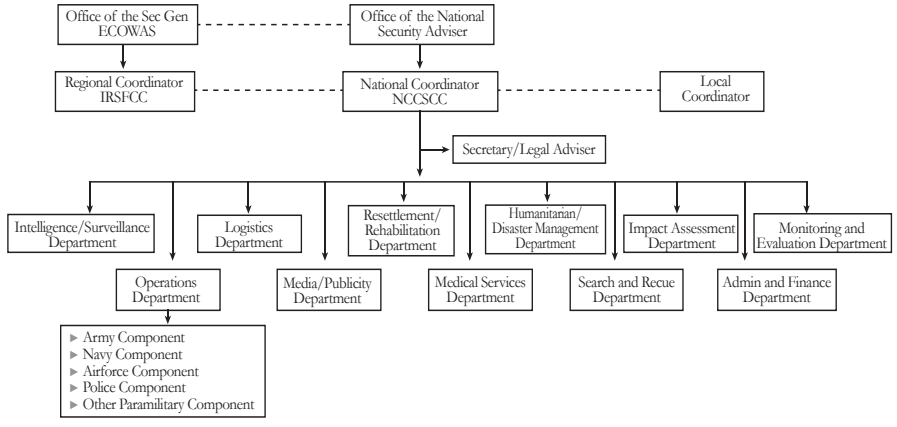
the complex interactions between social dynamics and climate change security issues in local communities. At the national and regional levels, well-trained and equipped security personnel may support diplomatic initiatives by cooperating with international agencies and bordering nations to develop coherent plans that address cross-border environmental problems. More so, West African states need to invest in local defence production to harness the potential therein as well as leverage international collaboration for technology transfer towards enhancing their defence industry.

Formulation of a Framework for Coordinating Stakeholders in Managing Climate Change-Related Security Activities. West African states could consider formulating a 'National Security Framework on Climate Change' (NSFCC) at the national level that would encompass the local level and an 'Integrated Regional Security Framework on Climate Change' (IRSFCC) at the regional level. The capacity to anticipate and avert possible security challenges arising from climate change-induced vulnerabilities and appropriate response measures would be at the core of these frameworks. The legislative frameworks shall provide the basis for establishing coordination centres at the national and regional levels as well as the funding mechanism for both the coordination centres and other climate change security-related activities. It would also strengthen the legislative frameworks for local communities' participation in climate-sensitive decision-making. Considering the complexities of these frameworks, existing national and regional security architecture frameworks should be leveraged to build consensus on their formulation and functionality under the purview of the Office of the National Security Advisers (ONSA) of respective countries and the Secretary General of ECOWAS respectively.

Establishment of a Coordinating Platform for Stakeholders in Managing Climate Change-Related Security Activities. One of the proposed revolutionary options to manage the complex security problems caused by climate change in West Africa is the establishment of a 'National Climate Change Security Coordination Centre' (NCCSCC) at the national level that encompasses the local level and a 'Regional Climate Change Security Coordination Centre' (RCCSCC) at the regional level as

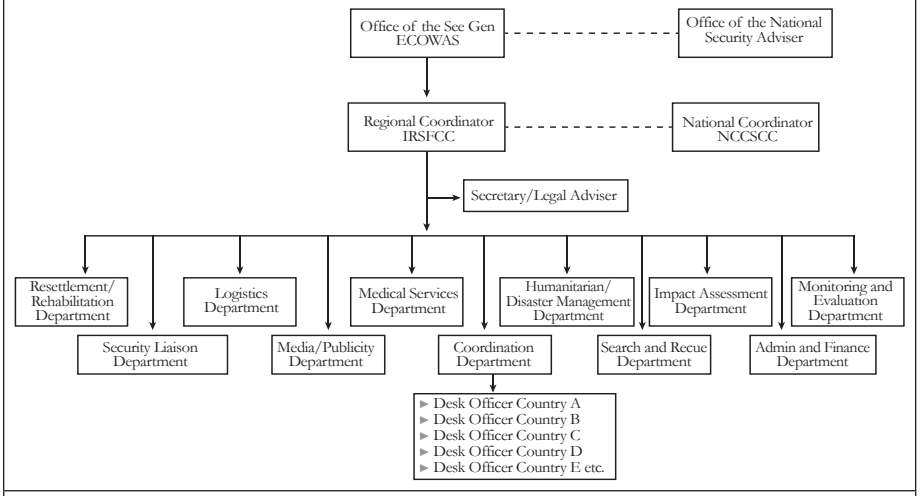
highlighted in Figures 8 and 9 respectively. The NSFCC and IRSFCC earlier proffered would provide the framework for the establishment of the NCCSCC and RCCSCC respectively. Similarly, the centres could rely on the ONSA of the respective member states and ECOWAS for their operationalisation. The centres would enable monitoring and early identification of vulnerable locations to resource disputes, migratory pressures, and societal instability through collaborative information and intelligence sharing as well as scenario planning between security and climate change management institutions. Decision-makers and security personnel may create targeted approaches to ease tensions before they become full-blown crises through such coordination centres. The centres would promote regional collaboration and diplomacy as they would lay the path for collaborative efforts to handle transborder environmental concerns by bringing parties from across international borders together. The centres shall coordinate cross-border disaster response and put into action harmonise national policies on climate change security-related activities. It would also promote regional dialogues on managing sustainable natural resources in transborder regions and protecting regional nomadic livestock migratory corridors.

Figure 8: Proposed Organogram of NCCSCC



Source: Author's Work

Figure 9: Proposed Organogram for IRCCSCC

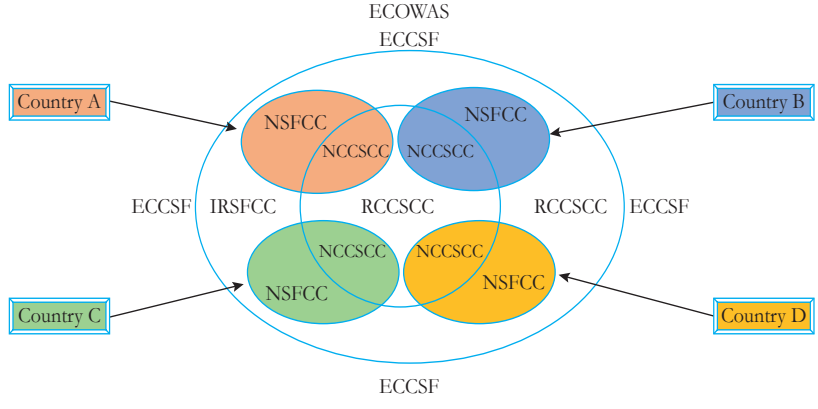


Source: Author's Work

Strengthening Governance of Managing Climate Change Security-Related Activities. The governments of West African states need to improve their commitment and socio-political will to execute and follow through with climate change reduction initiatives. It, therefore, beholds the governments to strengthen all relevant institutions in this regard. One such effort will be re-designating the nomenclature of the concerned ministries to include the word 'Climate Change'. While acknowledging, that the name change may not guarantee the desired commitment, it would, however, demonstrate the desired effort in securitising climate change that would help to influence and reawaken national consciousness on climate change and security-related challenges. Governments should also help bridge national legislation and traditional heritage in community policing and the justice system as well as between scientific and local knowledge gaps in mitigation and adaptation of climate change conflict-sensitive measures and strategies. Community inclusiveness should be promoted in the climate change decision-making process by developing local research capacity and inculcating the same into the national climate policy. Considering the paucity of funding, a flexible and enduring funding mechanism could be advocated for the region by establishing an ECOWAS stabilisation fund for

climate change-related security challenges, to be known as the 'ECOWAS Climate Change Security Fund' (ECCSF). To ensure the effectiveness and efficiency of this novel regional initiative, it is important to synergise all local, national, and regional level efforts through an integrated security architecture to be designated as the West Africa Climate Change Security-Related Architecture (WACCSRA) as shown in Figure 10 This proposed concept is not meant to be a stand-alone security initiative in the region but shall be inculcated as an integral part of the overall security effort of ECOWAS and member states. However, it is pertinent to state that to achieve this, West African states must adequately securitise climate change and incorporate democratic tenets to ensure political stability and good governance. This would ensure the required commitment and political will that will help to drastically reduce the spate of climate change-related security challenges in the region.

Figure 10: Proposed Organigram of WACCRA



Legend

NSFCO	- National Security Framework on Climate Change.
IRSFOC	- Integrated Regional Security Framework on Climate Change.
NOCSCC	- National Climate Change Secunty Coordination Centre.
ROCSCC	- Regional Climate Change Security Coordination Centre.
ECOWAS	- Economie Community for West African States.
ECOSF	- ECOWAS Climate Change Socurity Fund.
WACCSRA	- West Africa Climate Change Secunty Architecture.

Source: Author's Work

Recommendations

Consequently, the study recommends that governments at the local level should invigorate the traditional heritage of local policing, dispute resolution justice system and community-based adaptation to climate change. At the national level, the government should facilitate the formulation of NSFCC, the establishment of NCCSCC as well as the re-designating the nomenclature of concerned ministries to include the word 'Climate Change'. At the regional level, ECOWAS should facilitate the formulation of IRSFCC and the establishment of RCCSCC and ECCSF.

Conclusion

Climate change has become an important global issue of great concern due to its devastating impact on humanity. Its indirect link to complex and multifaceted security-related challenges in West Africa is undoubtedly germane and well-established by this study. This is more so as the peculiarity of West Africa's other inherent challenges therein, such as ungoverned spaces, weak state institutions, political instability, and policy inconsistencies, presents a more severe and challenging dimension to the issue of climate change-related security challenges, which are the core elements of the region's security challenges. Consequently, some challenges were identified and ways of tackling such challenges within the context of WACCSRA were proffered which are achievable through adequate securitisation of climate change and incorporating democratic tenets to ensure political stability and good governance by West African states.

References

1. Baumeister, R.F. & Vohs, K.D. (2007), "Realistic Group Conflict Theory". Encyclopedia of Social Psychology. 2: 725–726.
2. Blanche Verlie, 2022, Learning to live with climate change: From anxiety to transformation, Routledge, p.140. ISBN 9781-0320-7366-8.

3. Brown, Oli, Anne Hammill and Robert McLeman., 2007, "Climate change as the 'new' security threat: implications for Africa", International Affairs, Vol. 83, No. 6, pp.1141–1154.
4. Buzan, B. (2003). Regions and Powers: The Structure of International Security, Cambridge University Press.
5. CIA World Factbook, 2022.
6. Ebimboere Seiyefa (2019), How climate change impacts regional security in West Africa: Exploring the link to organised crime, African Security Review.
7. Food and Agriculture Organization (FAO) (2021), Nigeria Water Profile, New York: United Nations, National Bureau of Statistics 2021 Social Statistics, Abuja.
8. Homer-Dixon, 2017, "Environmental Scarcities and Violent Conflict".
9. Intergovernmental Panel on Climate Change Report (IPCC) for 2022.
10. Jibrin AT (2020), 'Synergy Among Key Security Agencies: A Panacea to Internal Security Crises', lecture presented to NDC Nigeria.
11. Blanche Verlie (2022), Routledge Learning to live with climate change from anxiety to transformation, 2022.
12. Marshall Burke, Katharine J. Mach (2019), "Climate as a risk factor for armed conflict".
13. Megan Duzor and Brian Williamson | VOA News, Coups in Africa by Numbers.
14. ND-GAIN Report for 2021.
15. Richard Matthew, Mark Zacher, 2016, 'Liberal International Theory, Common Threads, Divergent Strands'.
16. United States Environmental Protection Agency (USEPA) Annual view on greenhouse emission, 2021.

Author

Captain Musa Danjuma Jarma was commissioned into the Nigerian Navy as a Sub-Lieutenant on 17 September 2003 as a member of the 50th Regular Course of the Nigerian Defence Academy. The senior officer has a Bachelor of Science Degree in Chemistry, a Master of International Affairs and Defence Studies and a Master of Social Science in Security and Development. He has attended several military courses which include Sub-Technical and Long Courses (Navigation and Direction), Junior and Senior Courses at Armed Forces Command and Staff College (AFCSC) Nigeria as well as National Defence College Bangladesh. He has also attended several other professional courses, seminars, and conferences both within and outside Nigeria. The senior officer has held several operational, instructional and staff appointments in his career notably as a Directing Staff at the AFCSC Nigeria and a Military Observer in MONUSCO.

NDC JOURNAL
Security Through Knowledge

THE IMPACT OF SOCIAL MEDIA IN SHAPING MILITARY PUBLIC OPINION IN OMAN

Group Captain Rashid Hamdan Said Al Kalbani, ndc

Introduction

Social media refers to digital communication platforms that enable users to create, share or exchange information, opinions, ideas, pictures, videos, and other content in virtual communities and networks. Examples of social media platforms include Facebook, Twitter, Instagram, TikTok, YouTube, and LinkedIn (Alghamdi, 2020). Public opinion, on the other hand, refers to the collective attitudes, beliefs, and views held by a particular group or society about a particular issue, event, or phenomenon. Public opinion is shaped by various factors such as cultural norms, personal experiences, media exposure, and interpersonal communication. Public opinion plays a critical role in shaping political, social, and economic decisions and outcomes. Social media can play a significant role in shaping public opinion by amplifying and disseminating information and opinions, facilitating engagement and debate, and influencing the attitudes and behaviours of users (Alsaedi & Shukri, 2019).

In recent years, social media has become an important tool for shaping public opinion, particularly in the military sector. Oman is no exception, with its military, using social media to engage with its citizens and create a positive public image. The impact of social media in shaping military public opinion in Oman is an important area of research that can shed light on the effectiveness of social media in shaping public opinion in a non-Western context (Alghamdi, & Al-Rawahi, 2019).

Oman is a Middle Eastern country located on the south-eastern coast of the Arabian Peninsula. It has a long history of military service, with the Sultanate of Oman Armed Forces being established long time ago. Since

then, the military has played a key role in the country's development and stability. Oman has a relatively small population of around 5 million people, with a significant portion of its citizens being involved in the military. Social media has become a popular tool for Oman's military in shaping public opinion. Social media platforms such as Twitter, Facebook, and Instagram are used to provide updates on military operations, showcase the military's capabilities, and engage with citizens. Oman's military has also launched several social media campaigns to promote its image and increase its popularity among citizens.

The impact of social media in shaping military public opinion in Oman is an important area of research due to the unique cultural context of the country. Oman is a conservative Islamic society that values traditional social norms and values. Social media is a relatively new phenomenon in the country, and its use has been limited by traditional cultural norms. Therefore, understanding how social media is used to shape public opinion in this context is important for understanding the effectiveness of social media in non-Western cultures.

Review of Literature

Social media has emerged as a significant factor in shaping public opinion in various contexts, including the military. Numerous studies have explored the impact of social media on public opinion, but there is a lack of research on this topic in the context of Oman. This literature review provides an overview of the existing research on the impact of social media on military public opinion and highlights the need for further research in the Omani context.

Several studies have found that social media can have a significant impact on military public opinion. For example, a study by Sandoval-Almazan, R., & Gil-Garcia (2019) found that social media can enhance the transparency and accountability of military institutions and can also facilitate citizen participation in military decision-making. Similarly, a study by Cheong

and Lee (2020) found that online news sources can shape public attitudes towards the military by influencing the framing of news stories.

Other studies have focused on the role of social media in shaping military public opinion during times of conflict. For instance, a study by Chadwick and Howard (2018) found that social media can provide a platform for citizen journalism and can influence public opinion in favor of or against military intervention in conflicts. Similarly, a study by Khamis, Ang, and Welling (2017) found that social media can have a significant impact on the attitudes and opinions of military personnel towards military interventions.

Al-Najjar and Abualoush (2020) conducted a literature review on the use of social media by the military and found that social media plays an important role in shaping military public opinion. Similarly, Al-Saadi and Al-Khatri (2018) examined the role of social media in shaping public opinion in Oman and found that social media has a significant impact on public discourse and the government's ability to shape public opinion.

Research conducted by Nawazkhan, M, & Al-Qalhati , F (2022) investigated the global impact of social media on military public opinion. Their study revealed that social media platforms have become essential channels for the dissemination of military-related information and opinions. They found that these platforms can shape public sentiment, influence perceptions of military actions, and facilitate the spread of propaganda. Additionally, they highlighted the role of social media in mobilizing public support for military endeavors on a global scale.

A study by Al-Badi, Tarhini, & Al-Bolushi, 2020 explored the regional dynamics of social media's impact on military public opinion in the Gulf Cooperation Council (GCC) region, including Oman. Their findings indicated that social media platforms play a vital role in shaping public narratives and fostering discussions related to military activities. The study revealed that citizens in the region utilize social media to voice their opinions, engage in debates, and access alternative perspectives on military affairs.

Research Methodelogy

The research method employed is qualitative in nature and encompasses the following:

Research Design: The research design employs a qualitative framework to delve into the nuanced interactions between social media engagement and military public opinion formation in Oman.

Data Collection: The data collection outlines a mixed-method approach, using in-depth interviews and survey as primary data collection to explore individual experiences and broader patterns of social media's impact on military public opinion. Secondary data will be generated from published research studies, reports, and social media data analysis.

Discussion and Analysis

Across the globe, countries are diligently refining their competencies within this sphere. This social media imprint acts as a diplomatic tool for nations, casting their influence both at home and abroad. The ambition is to consolidate a significant position in global affairs, champion the freedom of speech, and ensure access to information. However, during periods of unrest, there is an imperative to regulate the flow of information to counteract social media inaccuracies, challenge the informational hegemony of major nations, and resist intentional disinformation campaigns. Recognizing this, Oman remains steadfast in its commitment to upholding both domestic and international security, confronting any elements that might sway public opinion. This commitment coexists with the imperatives set by the unyielding march of technological and societal change. Currently, the proliferation of varied social media platforms and channels is particularly noteworthy.

To achieve the research objectives, structured interviews were organized with representatives from public sectors, spanning government departments and defense entities. The aim was to delve into the tangible

impact of social media on shaping public opinion in Oman. Interview questions were designed to echo the core aims and challenges of the study, emphasizing foundational principles delineated in the research method related to diverse facets of public opinion, which include political, economic, societal, cultural, media, security, and military dimensions.

Dynamics of Social Media Engagement in Omani Society

The use and dependence on social media within Omani society are consistently increasing. Social media has emerged as a potent and sometimes controversial force, driving significant changes that deeply resonate with their daily experiences, thereby influencing public opinion in Oman. This influence is evident in the sheer volume of information and news shared, ranging from credible to dubious, and from unbiased to both inadvertently and deliberately skewed perspectives. These narratives span social, economic, political, and intellectual realms. In such a setting, social media has the capability to reshape specific trends and inclinations, or tilt public sentiment towards specific topics, necessitating rigorous oversight and continual review. Regardless of whether its impact is negative or positive, the implications of social media on Omani society and public opinion (as per the study sample) are detailed as follows:

The Negative Impact of Social Media on the Omani Society

One of the interviewee articulates concerns about the potential misuse of the vast connectivity offered by social media. He contends that it can be manipulated to threaten facets integral to a cohesive society, especially national unity. He mentions the potential for inciting tribal and sectarian divisions, promoting warped extremist ideologies, and the rampant spread of propaganda and unfounded rumors. This cascade of misinformation has the potential to breed unrest, diminish trust in the state and its institutions, and compromise the very ethical and religious values that form the bedrock

of the society. Expanding on this, another participant, emphasizes the challenges that rapid social media growth poses to the traditional Omani media education value system. There's a palpable tension between classical media outlets and the unrestrained nature of social media, which often operates devoid of consistent ethical standards or clear regulations. This expansive platform, influenced by both local and foreign narratives, can either unknowingly disseminate misleading content or intentionally undermine the very fabric of Omani society. This is accomplished by targeting its stability and cohesion through deceptive narratives, impacting various sectors, including the economy, culture, identity, and national unity. Recent national events have underscored the significants way social media holds over societal perceptions of critical national matters.

The Positive Influence of Social Media on Omani Society

Among the positive instances of the new media's impact are the initiatives undertaken by governmental entities within the Sultanate, as well as the business and investment sectors. These bodies have harnessed such platforms to achieve national objectives. Swiftly, the security and military apparatuses leveraged the new media optimally to counter rumors jeopardizing national security by disseminating security awareness, legal culture, combatting cybercrimes, and gauging public opinion concerning the services provided by the state.

The digital space is instrumental in fortifying values of loyalty and affiliation, fostering a positive sentiment towards the homeland and leadership, emphasizing the preservation of national achievements, highlighting government efforts, supporting positive views, and counteracting any attempts to tarnish or be little national accomplishments.

Social media has undeniably become a robust platform for communication and engagement across various sectors, including the military. In the context of Oman, it has notably influenced the strategic communication efforts of the military in several ways.

Firstly, social media allows for a direct channel of communication between the military and the public. This has been instrumental in disseminating accurate and timely information, thereby fostering transparency and trust. For instance, official military accounts on platforms like Twitter and Facebook provide updates on military exercises, humanitarian aid distributions, and other significant events, which are easily accessible to the public.

Secondly, social media has facilitated a broader dialogue and engagement. The interactive nature of social media enables the military to receive feedback and address concerns in real-time, which is crucial for maintaining a positive public perception and ensuring an open line of communication.

However, the openness of social media also presents challenges. The risk of misinformation and the spread of unverified information can potentially harm the military's image and create public relations crises. Additionally, security concerns surrounding sensitive information being shared on social media platforms are paramount.

Impact on Social and Cultural Security

This has manifested through the influence of new media on the emerging generation of Omani society. There is a looming threat of the virtual world overpowering reality, potentially leading, if unaddressed, to societal disintegration. This is primarily evident in weakened familial bonds, threatening the family's influence over children's behavior and exacerbating a lack of motivation to change or improve behavior. Much of this media content doesn't align with the values and culture of the Omani society and often contradicts Omani identity. This was exemplified by the case of female activists on social media platforms who propagated values and ideas foreign to the esteemed morals and noble values inherent in Omani society. However, on the flip side, such media can play a pivotal role in elevating the intellectual awareness of society across all domains, especially if a progressive national strategy is devised in tandem with this media's evolution, adapting its features to achieve such an objective.

It has been stated that there are several challenges the military faces when interacting with the public on social media platforms. Social media platforms can be rife with misinformation and disinformation, which can distort the public's perception of military actions or policies. It can be a challenge for military organizations to correct misinformation and maintain a factual narrative. Security is a paramount concern for military organizations. There's a risk of sensitive information being leaked or shared on social media platforms, which could potentially compromise operational security. Social media platforms provide a space for open discussion, which can expose military organizations to public criticism and negative feedback. This can be a challenge to manage, especially if it affects the morale of military personnel or the public's perception of the military. The anonymity that social media platforms can provide might lead to individuals sharing unauthorized or inaccurate information about military matters without facing immediate consequences.

Impact on Media Security

The advent of social media has disrupted the value system of Omani media education. A heated race between traditional and new media has emerged, crystallizing in the combat against rumors, misinformation, and false news. The vast freedom exercised on social media raises questions about its impact on the fate of official media discourse. The Omani society, like others, has varied educational and cultural levels, reacting differently to opinions of activists and community leaders regarding governmental decisions and legislations. This threatens to fragment national allegiance standards. This is exacerbated by the fact that social media has eroded many media concepts like credibility, reliability, and news sourcing, leading to the rise of media deception and misinformation, occasionally influencing public opinion to a degree that undermines national sovereignty. This was apparent in some cases of public dissent against state decisions and mistrust in its announced plans. The protests by job seekers in May 2021 across several provinces exemplify this reality, where official media could

not preemptively address virtual mobilizations, effectively educating and convincing society about pre-established governmental plans. These protests nearly escalated to a national security issue. On a positive note, the Omani government has commendably tried to strengthen its tools in the realm of new media, using its platforms to maintain Omani media identity, values, national achievements, and accomplishments. It aims to adopt a sophisticated policy to counter threats posed by this media, considering the importance of inoculating the Omani society from media influence through educational curricula, leveraging its features to promote media and cultural awareness.

It is noted that when establishing coherent policies and strategies for effective military public opinion control, several essential factors must be considered, including; establishing a culture of transparency and accountability is essential to fostering public trust. Regarding their activities, missions, and decision-making processes, military organizations should provide accurate and timely information. Effective policies involve proactive engagement with journalists and media entities in order to ensure accurate reporting and a balanced portrayal of military activities. Regular press briefings, interviews, and access to military personnel can assist in shaping public opinion.

Military organizations should engage actively with local communities and demonstrate their commitment to their well-being. Collaborative initiatives, such as community service projects, open houses, and public events, can cultivate positive relationships and increase public comprehension between the military and the general populace. Furthermore, implementing educational programs and public outreach campaigns can help to inform the public about the mission, values, and contributions of the military. These initiatives can dispel misconceptions, provide context for military operations, and highlight the professionalism and dedication of military personnel. Utilizing social media platforms and sustaining a strong online presence can be crucial for influencing public opinion. Military personnel should be provided with clear guidelines and training on social media use etiquette.

Ministry of Information has embarked on establishing a structured foundation for the operations of social media (new media). They remain committed to finalizing the legislative aspects related to publication guidelines and the specific media content within the Sultanate. The role of social media in the military's engagement with the public in Oman could potentially evolve in several ways: enhancing transparency, promoting positive interactions, educating the public on military activities, and managing public perception. It might also serve as a recruitment platform and a channel for real-time communication during crises. However, the trajectory would significantly depend on the policies adopted by the Omani military and the broader socio-political context in Oman. For a precise outlook, monitoring official communication and developments concerning military-social media engagement in Oman would be crucial.

Survey Analysis

This research aimed to investigate the influence of social media on shaping public opinion regarding the military in Oman. A survey was conducted with 234 participants to gather insights into their perceptions and experiences related to the topic. The following analysis summarizes the key findings based on participant responses.

Social Media's Influence on Perception of the Military. The majority of participants (over 90%) agreed that social media platforms have significantly influenced their perception of the military in Oman. This suggests that social media plays a substantial role in shaping public opinion in the context of the Omani military.

Encounter of Military-Related Information on Social Media. A significant number of respondents indicated that they frequently encounter information related to the military on social media platforms in Oman. This highlights the prevalence of military-related content in the digital space and its accessibility to the public.

Positive Influence on Public Opinion: A noteworthy finding is that a substantial majority of participants believe that social media has had a positive impact on public opinion towards the military in Oman. This suggests that the Omani military has effectively used social media to project a favorable image and engage with the public.

Influence on Shaping Opinion About Military Operations. A significant proportion of respondents (over 91%) indicated that social media has been highly influential in shaping public opinion about military operations and activities in Oman. This underscores the importance of social media as a platform for disseminating information and engaging with the public regarding military activities.

Improved Understanding between the Military and the Public. A majority of participants believe that social media has played a role in improving the understanding between the military and the general public in Oman. This indicates that social media has been an effective tool for fostering transparency and communication between the military and civilians.

Effective Utilization of Social Media by the Military. Participants generally perceived that the military in Oman highly effectively utilizes social media to communicate with the public. This suggests that the Omani military has successfully leveraged digital platforms for public outreach and engagement.

Influence on Perception of Military Capabilities. A significant number of respondents indicated that social media has highly influenced their overall perception of the military's capabilities and readiness in Oman. This implies that the military's digital presence has contributed to shaping public confidence in its abilities.

Limited Negative or Critical Information. A noteworthy observation is that participants rarely encounter negative or critical information about the military on social media platforms in Oman. This could indicate that the military's messaging on social media tends to be positive and well-received.

Based on the survey findings, it is evident that social media plays a substantial role in shaping public opinion regarding the military in Oman. The Omani military has effectively used social media to project a positive image, engage with the public, and influence perceptions about its capabilities and activities.

Research Findings

The relationship between social media and military public opinion refers to the interaction and influence that social media platforms have on influencing the attitudes, beliefs, and perceptions of individuals within the military community as well as the public regarding military-related issues. The social media provide a forum for the dissemination of information, discussions, and debates that have the potential to substantially influence public opinion on military matters. This understanding reveals how social media platforms influence the formulation and evolution of military public opinion.

Social media play a significant role in shaping military public opinion by providing a forum for information exchange, participation, and discussion. It can influence the attitudes and beliefs of military personnel by exposing them to diverse content, perspectives, and discussions on military affairs. Social media platforms have the ability to reinforce existing beliefs, challenge preconceived notions, and provide access to diverse perspectives. By analyzing the impact of social media on the beliefs and attitudes of military personnel, we can gain insight into how social media contributes to the formation and evolution of their opinions.

To effectively navigate the challenges and capitalize on the opportunities presented by social media in the context of military communication, effective policies and strategies are required. This question seeks to identify and develop policies and strategies that resolve the challenges posed by social media, such as misinformation, security concerns, and maintaining a unified message. In addition, it examines strategies for maximizing the

use of social media platforms, such as nurturing transparency, public engagement, and trust, as well as leveraging social media analytics for insights and adapting communication strategies accordingly. In the digital age, coherent policies and strategies assure a consistent and strategic approach to military communication.

Recommendations

Based on the analysis and conduct of the study, the researcher proposes the following recommendations:

Further Analyze the Specific Impacts. Conduct in-depth research to investigate the specific effects of social media on Oman's military public opinion. This could entail studying the patterns of information consumption, examining the relationship between social media engagement and the attitudes/beliefs of military personnel, and investigating the factors that influence public opinion on military matters through social media.

Explore the Effectiveness of Different Communication Strategies. Examine and compare the efficacy of the various communication strategies utilized by military organizations in Oman. This may involve evaluating the impact of various content formats, messaging strategies, and engagement techniques used on social media platforms. By analyzing and contrasting these strategies, insights into what resonates most effectively with military personnel and the public can be gained.

Assess the Perception Gap. Determine the perception disparity between military personnel and the public concerning military issues. This involves investigating how social media influences the divergence or convergence of these two groups' attitudes and beliefs. Understanding the perception gap can inform the development of targeted communication strategies and provide insight into the challenges of effectively shaping military public opinion.

Evaluate the Impact of Social Media on Trust and Confidence. Investigate the effect of social media on the Omani military's trust and confidence. This could involve investigating the relationship between social media participation, openness, and public confidence. Understanding how social media influences levels of trust can assist in the development of communication strategies that increase public confidence and strengthen the relationship between the military and the public.

Assess the Role of Influencers. Examine the role of influencers, both internal and external to the military community, in shaping military public opinion in Oman. Analyze the impact of influential figures on social media platforms on attitudes, beliefs, and perceptions regarding the Omani military. Understanding the influence of these individuals can inform collaboration and engagement strategies with influencers to amplify positive narratives and combat misinformation.

Develop Guidelines and Policies. Develop comprehensive policies and guidelines for the effective and responsible use of social media in Oman's military organizations. This includes addressing security concerns, preserving operational confidentiality, and ensuring messaging consistency while allowing for individual expression. Developing clear guidelines and policies assists in mitigating potential risks and maximizing the benefits of social media in influencing military public opinion.

Longitudinal Studies. Conduct longitudinal studies to monitor the evolution of military public opinion because of social media influences over time. This can provide insight into trends, shifts, and the efficacy of the military's communication strategies. Longitudinal studies can assist in recognizing long-term patterns and adjusting communication strategies accordingly.

Conclusion

This study investigated the influence of social media on Oman's military public opinion. Several important conclusions are reached by analyzing existing knowledge and hypothetical research results.

The influence of social media on the formulation and shaping of military public opinion in Oman is substantial. It influences the attitudes, beliefs, and perceptions of both military personnel and the public.

Complex and multifaceted is the relationship between social media and military public opinion. Contributing to the evolution and formulation of public opinion, social media platforms offer the chance to interact with a variety of content, perspectives, and discussions concerning the Omani military.

Social media's influence on military public opinion extends to the attitudes and beliefs of military personnel. The exposure of military personnel to a variety of perspectives, discussions, and information on social media can potentially shape their attitudes and beliefs about the Omani military.

Effective policies and strategies are essential for utilizing social media in military communication effectively. With clear guidelines, training programs, crisis communication frameworks, and transparent practices, military organizations can navigate the challenges posed by social media platforms and capitalize on the opportunities they present.

The challenges of misinformation, security concerns, managing public perception, and addressing biases must be acknowledged and addressed on social media platforms. Consistent policies and strategies should consider these obstacles and include measures to combat misinformation, ensure security, maintain transparency, and close communication gaps.

By continuously studying and adapting to the evolving landscape of social media, military organizations in Oman can optimize their communication efforts, enhance public trust, and effectively shape military public opinion in alignment with their organizational goals.

References

1. Al-Azri, N., & Al-Gharbi, K. (2016). The Impact of Social Media on the Public Opinion and the War on Terrorism in Oman. Journal of Communication and Media Technologies, 6(2), 98-106.

2. Al-Jenaibi, B., & Al-Mahruqi, R. (2019). Social Media and the Omani Public Sphere. Journal of Arabian Studies, 9(2), 161-177.

3. Al-Jumaily, A. (2018). The Role of Social Media in Shaping Public Opinion in Iraq. Journal of Political Science and International Relations, 1(1), 1-10.

4. Al-Najjar, F., & Abualoush, S. (2020). The Use of Social Media by the Military: A Review of the Literature. Journal of Military Studies, 11(1), 1-18.

5. Al-Rawi, A., Al-Khalifa, H. S., & Al-Shehabi, S. (2016). Social media and public opinion: A study of Bahrain's "Arab Spring". Journal of Arab & Muslim Media Research, 9(2), 159-175.

6. Al-Saadi, A., & Al-Khatri, M. (2018). The Role of Social Media in Shaping Public Opinion in Oman. Journal of Public Administration, Governance and Law, 11(2), 168-184.

7. Alghamdi, A., & Al-Rawahi, N. (2019). The impact of social media on political participation and public opinion in Saudi Arabia. Global Media Journal, 17(33), 1-15.

8. Alsaedi, M., & Shukri, R. (2019). The influence of social media on public opinion in Kuwait. International Journal of Advanced Computer Science and Applications, 10(6), 160-165.

9. Al-Badi, A., Tarhini, A., & Al-Bolushi, H. (2020). Adoption of social media for public relations professionals in Oman. ICT for an Inclusive World: Industry 4.0–Towards the Smart Enterprise, 229-247.

10. Al-Harthi, S. (2018). The role of traditional media in shaping public opinion in Oman. International Journal of Social Sciences and Humanities Research, 5(1), 35-42.

11. Al-Kalbani, A. (2019). The role of media in shaping public opinion: A case study of Oman. International Journal of Applied Business and Economic Research, 14(4), 2359-2374.

12. Al-Rawi, S. (2022). Social media in the Arab world: Leading up to the uprisings of 2011. Westminster Papers in Communication and Culture, 9(2), 11-34.

13. Al-Saggaf, Y. (2019). Social media in the Arab world: Influences and constraints. International Journal of Communication, 2932-2951.

14. Amedie, J. (2020). The impact of social media on society. International journal of computer sciences and engineering 5.10, 55-60.

15. Bu-salim, A. (2019). Oman: Economic, social and strategic developments. Issue paper 4 , 2019.

16. Chadwick, A., & Howard, P. N. (2018). The Routledge handbook of Internet politics. Routledge.

17. Dong, X., & Ying Lian. (2021). review of social media-based public opinion analyses: Challenges and recommendations. Technology in Society 67, 101724.

18. Hayes, C. (2019). Realizing the social internet? Online social networking meets offline civic engagement. ournal of Information Technology & Politics, 6(3-4), 197-215.

19. Khafaga, S. A. (2021). n exploration of perceptions and use of misinformation on the social Web in Oman. Global Knowledge, Memory and Communication , 66-74.

20. Khan, F. R. (2019). Investigative study of preferred social media marketing in Safeer Mall, Sohar, Oman. Humanities & Social Science Reviews 5.1 , 53-63.

21. Mbaga, M. D. (2019). Social cybersecurity: an emerging national security requirement. Military review 99.2, 117.

22. McGregor, S. (2019). Social media as public opinion: How journalists use social media to represent public opinion. Journalism 20.8, 1070-1086.

23. Romer, P. (2020). Social media and political activism in the Arab world: Implications for public opinion and political behavior. Journal of Applied Security Research, 8(3), 305-326.

24. Samuel, B. S., & Sarprasatha, J. (2019). Entrepreneurship in social-media services in Oman: a socioeconomic scanning of the sultanate. Asian Social Science 12.4, 138.

25. Simplício, A. H. (2020). Social media and Dentistry: ethical and legal aspects. Dental press journal of orthodontics 24, 80-89.

Author

Group Captain Rashid Hamdan Said Al Kalbani, born in August 1975 in Oman, joined the military in 1994 and commissioned in 1996. This promotion landed him a significant position in the Security Directorate of the Royal Air Force of Oman. He enriched his military knowledge through various courses, both in Oman and overseas, enhancing his service to his nation. Rashid has held diverse roles within the Air Force, including command, staff, and training appointments, significantly contributing to its operations. He led security wings in air bases and a ground defense training squadron in the Sultan Qaboos Air Academy. His tenure in two different ranks, flight commander and squadron leader, showcases his progressive military journey. Through dedication and continuous learning, Group Captain Rashid has been an exemplar of service and a valuable asset to the Air Force.

NDC JOURNAL
Security Through Knowledge

INDIGENOUS DEFENCE INDUSTRY THROUGH REVERSE ENGINEERING: A DRIVE TOWARDS SELF-SUFFICIENCY FOR BANGLADESH ARMY

Colonel K M Mehedi Hasan, afwc, psc

Introduction

Every nation must protect its sovereignty, territorial integrity, and interests essential to national security. According to Adam Smith, the prime duty of the 'sovereign state' is to protect its society from violence and invasion by a standing military force - conscripted or professional. As such, the nation-states' responsibility is to build, prepare, maintain, and employ a military force in peace and war. (Narain & Datta; 1989 cited in Islam, 2010). While security issues continue to pose newer challenges in the Volatile, Uncertain, Complex and Ambiguous (VUCA) environment, nations must prepare their armed forces for war by all means. Thus, the production or acquisition of defence hardware remains a perpetual necessity (Islam, 2010).

Self-sufficiency in defence production is a prerequisite for being militarily effective. Self-sufficiency in arms production brings strategic autonomy, especially in times of crisis. There are two models of military hardware production: import-substitution and export-oriented. Under these two basic models, broadly four different strategies are available for producing defence hardware: Indigenous Production with Native Design, Transfer of Technology (TOT), Joint Venture (JV), and Reverse Engineering (Noman, 2020). Each has inherent strengths and weaknesses, especially for high-end defence production. The capacity to design and develop new weapon systems demands high R&D costs, which remains a challenge for most developing countries like Bangladesh. TOT may not be a viable option in the rapidly changing technology and commercial cost-benefit analysis of the Original Equipment Manufacturer (OEM) business environment.

Huge technological and currency differences may put Bangladesh in a disadvantageous position in the case of JV. In that context, Reverse Engineering remains a viable option for indigenous defence production. However, the Bangladesh Army has yet to materialize any of the options for the indigenous development of capital equipment to attain self-sufficiency.

The current regional and extra-regional geo-strategic relationship does not assure defence support in times of crisis (Alam, 2011 cited in Noman 2020). Sensing reality, contemporary armies have made substantial progress in their defence production. In contrast, the Bangladesh Army is yet to make mentionable progress in defence production. Considering all these, this paper attempts to identify the feasibility of Reverse Engineering as a method of indigenization. Upon doing so, it figures out how best Reverse Engineering can be adopted in the Bangladesh Army overcoming the challenges ahead. A sustained roadmap is also recommended at the end.

Methodology

The paper primarily looked at how Reverse Engineering can help in establishing indigenous defence industries for the Bangladesh Army. A deliberate study was carried out to find out the answer mostly by qualitative analysis. However, quantitative analysis substantiated the findings. Random sampling was done from mid and senior strata of leadership from various arms and services. A structured questionnaire was circulated for the survey. Collected responses were processed through Microsoft Excel for descriptive analysis. Various books, publications, articles, and unpublished papers were consulted as a part of the qualitative analysis. Consultation of various technical documents, data related to arms and equipment purchase at Army Headquarters, capacity and capability of various domestic industries were carried out. Key Informants' Interview (KII) and Focus Group Discussions (FGD) remain as primary source of information for this paper.

Paths to Indigenization: Reverse Engineering in Focus

Reverse Engineering is the process of designing, manufacturing and assembling products and systems. Reverse Engineering is the duplication of existing products. In general, 'Reverse Engineering' involves replicating a product by studying its makeup and structure. A few other approaches, accessible worldwide to achieve self-sufficiency in defence manufacturing, are Indigenous Production with Native Design, Transfer of Technology (TOT), and Joint Venture (JV) (Noman, 2020).

Rahman, 2023 argues that advanced countries will not be interested in TOT to Bangladesh unless they find it economically and socio-politically feasible. The socio-political scenario of Bangladesh has not been so stable that would have encouraged foreign countries to invest in Bangladesh for defence industries. More so, the transferred technologies, in most cases, are either obsolete or age-old (FGD 1).

Brigadier General Abu Naser (Retired), a security analyst, thinks that for a country like Bangladesh, defence industries must be economically viable. To make it economically viable, it has to be export-oriented. However, exporting military hardware does not go with our Export Policy 2018-2021. This issue seriously bars the idea of JV in Bangladesh (Rahman, 2023). Because, no country or tech-giants will be interested to set up a big plant in Bangladesh unless it will be economically viable through export. General Naser also argues that the best-suited solution is the combination of all methods, from which each can be carefully selected for a particular type of item.

In light of the previous discussions, a question was asked to most of the Key informants: instead of choosing one method for all the items, can the Bangladesh Army categorize the military hardware as per technical intricacies and choose an appropriate method for each category? The summary of the reply is appended below.

For high-end, technically advanced military products like electronic gadgets: TOT and JV.

For medium category and moderately advanced military arms, equipment, and vehicles: Indigenous Production with Native Design, and Reverse Engineering.

For low-end military products like personal gear: Indigenous Production with Native Design.

Feasibility of Reverse Engineering: Bangladesh Army Perspective

Legal Aspects of Reverse Engineering in Bangladesh

For Reverse Engineering, it is essential to know patent law, trademark rules, ordinances, and laws of the World Intellectual Property Organization (WIPO), World Trade Organization (WTO), and other procedural requirements. Before merchandising a product, it is required to acquire a patent for the product. Production and marketing of a technology by a person other than the patentee of this licensee during the lifetime of a patent is an infringement of the law. But if the patent life of the technology is expired or if it is not patented, then producing the product/technology through Reverse Engineering and marketing is not unlawful.

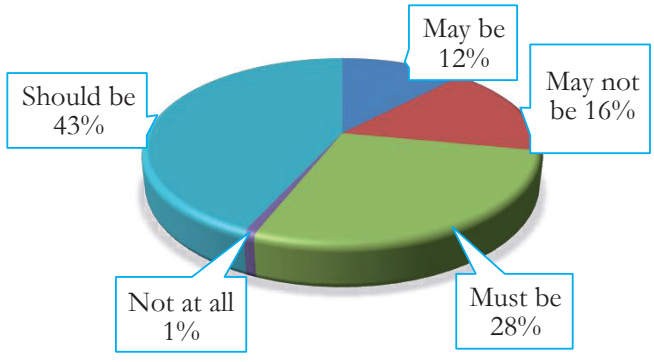
The next criterion for marketing a product at the national and international levels is to fulfill the requirements pertaining to the ordinance and law of WIPO and WTO as Bangladesh is a member of both organizations. However, patenting needs a public disclosure of an invention, and the need to submit the complete design to WIPO in a manner sufficiently clear and complete to enable it to be replicated by a person with an ordinary level of skill in the relevant technical field (WIPO Website). This often discourages the inventors of sophisticated military hardware from getting a patent from WIPO. Practically, there is hardly any arms, ammunition, or military hardware which is patented.

The US Supreme Court verdict says 'Legally, reverse engineering is deemed as a fair and honest means of starting with the known product and working backwards to divine the process which aided in its development or manufactures' (U.S. Supreme Court, 1974 cited in Wang, W., 2010). As such, Bangladesh can develop the Reverse Engineering practice keeping an eye on all notices pertaining to laws and ordinances of international proprietary rights systems. Selection of potential patent-expired or unpatented products/technology of developed countries or applying various modifications to an existing product/technology can be a policy in Reverse Engineering practice in Bangladesh.

Economic Viability of Reverse Engineering

The benefit of indigenization through Reverse Engineering lies in attaining self-sufficiency and Strategic Autonomy. However, it may not be economically viable because of the limited domestic market and restrictive export policy. Against that backdrop, Key Informants were asked whether the defence industries always need to be economically viable or not. Executive Chairman, BEPZA opined that for a country like Bangladesh, it is important that a defence industry in Bangladesh is economically viable. The present economic state of Bangladesh vis-à-vis the geo-political realities does not allow Bangladesh to set up economically non-viable defence industries. (Rahman, 2023). However, Engineer in Chief, Bangladesh Army thinks that defence industry may not be a money-earning industry. The profit remains with the sovereignty of the country (Salehin, 2023). A similar question floated to the survey respondents. The reply is reflected in Figure 1 where mostly it speaks that defence industries need to be economically viable.

Figure 1: Need of Defence Industries to be Economically Viable



Source: Survey

To check the economic viability, the author carried out a few case studies on already reverse-engineered products within Bangladesh. In 2015, BOF could successfully make artillery shells through Reverse Engineering. Besides Reverse Engineering, BOF also tried to make artillery shells in the Complete Knocked Down (CKD) method where all the components including the shell body were bought from abroad. In the CKD method, it was found that the cost is almost the same as the imported one. However, Reverse Engineering could save 37% on the same product. Similarly, 47% and 40% savings were made compared to import costs in producing 82 mm and 60 mm mortar bombs in BOF. Savings are even more in the case of mortar guns (AHQ Industrial Cell).

Technological Viability of Reverse Engineering in Bangladesh

Reverse Engineering is the process of analyzing and understanding the design, structure, and functionality of a product or system by deconstructing it. Technological advancements play a crucial role in facilitating Reverse Engineering processes and enabling efficient and accurate results (FGD 2). The following paragraphs will highlight the technological requirements for Reverse Engineering and then it will relate those requirements with the existing capabilities of different institutions in Bangladesh related to those fields.

3D Scanning and Imaging. 3D scanner serves as a foundation for Reverse Engineering, allowing engineers to analyze and recreate the object's design. So far, high-level precision 3D Scanning facilities are not available in Bangladesh (FGD 2).

Computer-Aided Design (CAD) Software. CAD software has evolved to provide sophisticated tools for Reverse Engineering. These software applications allow engineers to import 3D scan data, manipulate it, and convert it into editable CAD models. This is very well possible in Bangladesh, especially in institutions like Bangladesh University of Engineering and Technology (BUET) and MIST. Several private farms have trained manpower for 3D Modelling (FGD 2).

Additive Manufacturing (3D Printing). Additive manufacturing technologies, commonly known as 3D printing, have revolutionized the production of physical prototypes and parts. Engineer Tareq Monowaruzzaman, the Chief Engineer of a 3D Architecture and Design Farm informed that 3D printing is very common in Bangladesh. The facility is also there in MIST. The prototype of any parts of machinery (Within the size of 1 foot by 1 foot) can easily be produced (FGD 2).

High-performance Computing. High-performance computing (HPC) systems and cloud computing platforms provide the computational power necessary to process large amounts of data and perform resource-intensive tasks quickly. This capability enables engineers to analyze and Reverse Engineer complex systems efficiently. Big data analysis capable infrastructure and trained manpower are available in MIST (FGD 2).

Infrastructural Facilities Available for Reverse Engineering

State-Owned Technology Hubs/Facilities Run by the Bangladesh Army

Bangladesh Ordnance Factories (BOF). BOF is the country's first defence production facility built in 1970 with Chinese assistance. Last 50 years, BOF undertook several technical projects (BOF Website). Besides,

BOF conducted comprehensive research and development efforts, resulting in the successful production of various military products. BOF has a direct influence on the defence potential of our country. Taking the leverage of 53 years of experience in defence production, BOF can be the nerve centre for Reverse Engineering (FGD -1).

Bangladesh Machine Tools Factory (BMTF) Limited. Bangladesh Machine Tools Factory Limited is one of the largest industries of its kind in Bangladesh located at Gazipur. Government of Bangladesh handed over BMTF to the Bangladesh Army on 27 July 2000. Since then, BMTF in functioning as a state-owned limited company under the management of the Bangladesh Army with the motto of 'Production through Excellence' (BMTF Website). There are a total of 17 factories that are producing 1000 diversified and multidimensional types of products. The vehicle assembly section has the required facilities to reverse engineer military automobiles (Ahmed, 2023).

Bangladesh Diesel Plant (BDP) Limited. On 30 May 2007, this organization was handed over to the Bangladesh Army with the recommendation of the Privatization Commission through the Ministry of Defence (BDP Website). This factory specializes in assembling engines and engineering items. This factory also assembles battery-operated electric vehicles. The factory participates in the production and provision of essential equipment and replacement components for APC BTR 80 and tank MBT 2000 by utilizing the technique of Reverse Engineering.

Technology Hubs/Facilities within Army

901 Central Workshop EME. 901 Central Workshop is the only organization in the Army that has a dedicated Reverse Engineering lab. A modern electronics lab was inaugurated on 08 December 2021 by the Chief of Army Staff, Bangladesh Army. However, due to the lack of objectivity, this lab is yet to show any visible progress in the Reverse Engineering field (Ahmed, 2023).

902 Central Workshop EME. 902 Central Workshop was established in 1992, with a focus on tank production. Annually, it can conduct comprehensive maintenance and fundamental repairs for 50 tanks, field guns, and AD guns. The workshop possesses the capacity to manufacture 62 varieties of spare parts for tank engines and armaments, as well as 553 types of spare parts for tank hulls. Its infrastructure boasts substantial capabilities that could be harnessed for the production and assembly of heavy vehicles (Rasel, 2022). By incorporating some advanced machinery, it could potentially evolve into a center for Reverse Engineering.

Summary of Feasibility Analysis

The paper examined the viability of Reverse Engineering in Bangladesh from four angles: technological, legal, economic, and infrastructure-related. Reverse Engineering is highly connected to legal issues. A country like Bangladesh may suffer devastating consequences if any international rules and regulations are disregarded. However, the complexities of legal concerns can be avoided with rigorous study of patent law and, more importantly, with prudent item selection. Whether or not the defence sectors need to be financially lucrative is a hot topic of discussion. The study demonstrates that all reverse-engineered products in the Bangladesh Army were commercially viable, which is necessary for a country like Bangladesh.

Bangladesh still lacks the sophisticated technological prowess needed for Reverse Engineering. Poor R&D infrastructure, a lack of objectivity, and a tight budget all contributed to insufficient technological advancement. However, the Bangladesh Army is the owner of numerous industrial outfits with unrealized potential. The BOF, BMTF, and BDP can serve as the centre of Reverse Engineering for the Bangladesh Army once they are combined with military-run educational institutions like MIST and Bangabandhu Sheikh Mujibur Rahman Aviation and Aerospace University.

Challenges of Reverse Engineering

Incoherent Policies at Different Levels. Various policies concerning defence industrialization, more particularly production, import, and export of arms, ammunition, and defence hardware as promulgated by different government entities are quite incongruent and a barrier to the development of defence industries through Reverse Engineering. A few examples are appended below:

- The establishment of a formidable defence sector has been given significant attention in Defence Policy 2018, although no clear policy parameters have been laid down (Extract of Defence Policy 2018).
- National Industrial Policy 2016 has preserved weapons, ammunition, and other military equipment and machineries as a sector that is only reserved for state-owned enterprises.
- As per the Export and Import Policy 2015–20, the private sector is prohibited from engaging in the export or import of military-grade firearms, ammunition, and associated materials.

Limited Defence Budget. Bangladesh spends roughly 7%-8% of the entire national revenue on defence. Spending on the military is quite inadequate compared to what is needed for the armed forces. Pay, pensions, allowances, maintenance, and services take a major share of the defence budget. The usual amount spent on procurement or capital purchases is not sufficient for R&D required for Reverse Engineering (Hossain, 2023). The distribution of the budget in its current form makes it nearly impossible to build any kind of defence industry for Reverse Engineering.

Low Yearly Requirement of Arms, Ammunition, and Equipment. Except for small arms and small arms ammunition, the annual demand for armaments and ammunition during peacetime is fairly low. Therefore, the development of Reverse Engineering industries focusing only on meeting the requirement of the Bangladesh Armed Forces are unlikely to be economically viable (Salehin, 2023).

Lack of Public-Private Partnership. The private sector industries and factories that could effectively be integrated with the defence industries for Reverse Engineering have not yet been thoroughly studied or assessed. If there is a need, these could be of great help in building bigger industrial and technological bases for defence-related projects in the future (Naser, 2023).

Absence of a Central Body for Defence Production. There is currently no central body or organization in place to oversee, coordinate, and carry out various military equipment manufacturing projects for all three branches of the armed forces. In India, there exists a primary coordinating body referred to as the Department of Defence Production (DDP), operating within the Ministry of Defence. The main responsibility of the DDP is to establish an all-encompassing production framework aimed at manufacturing the necessary weaponry, systems, platforms, and equipment essential for safeguarding the nation. The Ministry of Defence Production in Pakistan and the Directorate of Defence Industries (DDI) under the Ministry of Defence in Myanmar perform the same role in Pakistan and Myanmar respectively (FGD 1).

Ways Forward for Reverse Engineering in Bangladesh

Make or Buy - A Strategic Directive. A strategic directive is necessary to prepare the road map to enhance defence production. Before developing the industry, the decision must be taken on how much Bangladesh should buy and how much should be produced locally (Salehin, 2023). Armed Forces Division (AFD) should take up a detailed study focusing on the prospects of the defence industry through Reverse Engineering in Bangladesh and approach the strategic leadership of the country.

Amendment of Existing Industrial and Export Policies. The private sector acts as a feeder organization for defence industries. However, without export potential, the defence industry cannot grow or maintain its viability from an economic standpoint. For a better future of Reverse Engineering within the country, the Industrial Policy 2016 and Export

Policy 2018-21 must be amended (Hossain, 2023). After meeting the domestic requirements, arms, ammunition, military equipment etc. can be exported to regional markets like Afghanistan, Bhutan, Nepal, Maldives Sri Lanka, etc.

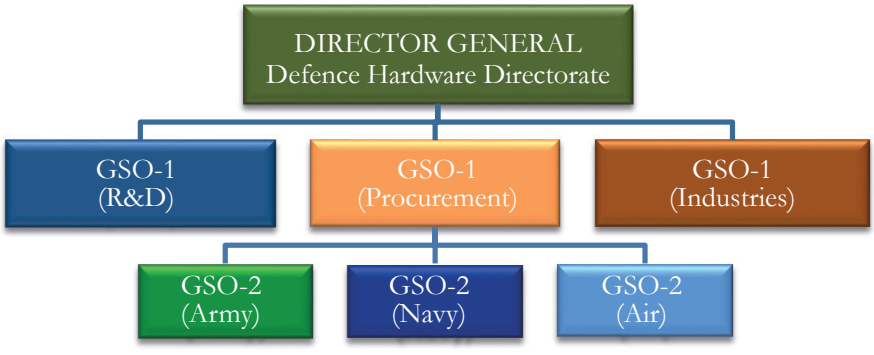
Reactivating Defence Science Organization (DSO). Defence Science Organization (DSO) was a government body under the Ministry of Defence (MOD). The government of Bangladesh closed this organization in the early '90s due to continuous poor performance in the field of R&D and reframed it as Space Research and Remote Sensing Organization (SPARSO). DSO may be reactivated, or such organization may be created under MOD or AFD and appropriate responsibilities may be specified. This body will be required not only to supervise and monitor any project but also to provide legitimacy and authoritative guidance for the R&D of various public and private establishments (AHQ Project Study Paper, 2010).

Categorization of the Products. Most of the Key Informants opined that the Bangladesh Army should categorize the defence hardware and equipment as High-end products which include technically advanced military hardware like electronic gadgets, Medium category and moderately advanced arms, equipment, and vehicle, Low-end military products like personal gear. To start with, the Army should target the second and third-category military products for Reverse Engineering. Medium and high-end products can be manufactured with TOT to achieve self-reliance within a short time (Rahman, 2023).

Establishing University-Industry Cooperation. University-industry cooperation or academia-industry partnership refers to the collaborative efforts between universities and industries to leverage their respective strengths and resources for mutual benefits. This collaboration aims to bridge the gap between academic research and real-world application by combining the knowledge and expertise of academia with the practicality and resources of the industry. Military-run technical institutions like MIST and industries like BOF or BMTF may have excellent cooperation for Reverse Engineering (FGD 2).

Formulation of Regulatory Bodies for Reverse Engineering Projects. An appropriate advisory body at the ministry level, an executive body at the AFD level and a working body at the services level are required for policy formulation, planning, execution and constant supervision of Reverse Engineering projects. Defence Science Organization (DSO) may be reactivated to strengthen the R&D at the national level and to derive technology from the private sector. An Executive Body named Defence Hardware Directorate (DHD) is to be formed at AFD level to coordinate the defence production and procurement of all three services. These regulatory bodies will be responsible to the Government/Army to ensure the timely implementation of projects and proper utilization of the resources. A proposed organization of the Defence Hardware Directorate (DHD) is appended in Figure 2.

Figure 2: Proposed Organization of the Defence Hardware Directorate (DHD)



Source: Author's construct

A Roadmap to Reverse Engineering Projects in Bangladesh Army

Enhancing and developing the capabilities of Reverse Engineering industries is a time-consuming aspect that needs deliberate planning and execution. In subsequent paragraphs, a roadmap of the Reverse Engineering concept is highlighted which is implementable within a timeframe of 4-5 years.

Step 1: Setting up Goals. At the very outset, it is imperative to set up a goal for the indigenous defence industry, Reverse Engineering in particular. The top brass of the country needs to articulate a vision of defence industrialization.

Step 2: Policy Formulation. At this stage, the industrial, export and import policy of the government will be reformed. Restrictions on arms export and public-private partnerships on defence production need to be lifted.

Step 3: Setting Up Management for Reverse Engineering Projects. Overall management in Reverses Engineering Industries can be configured into three levels: Top-level Management (Overall responsibility), Mid-level Management (Specific responsibility), and Lower-level Management (Production management). Creating a permanent Defence Industrial Coordination Directorate at AFD and an Inter-ministry Defence Industrial Coordination Body at MOD is of paramount importance for defence industrialization through Reverse Engineering.

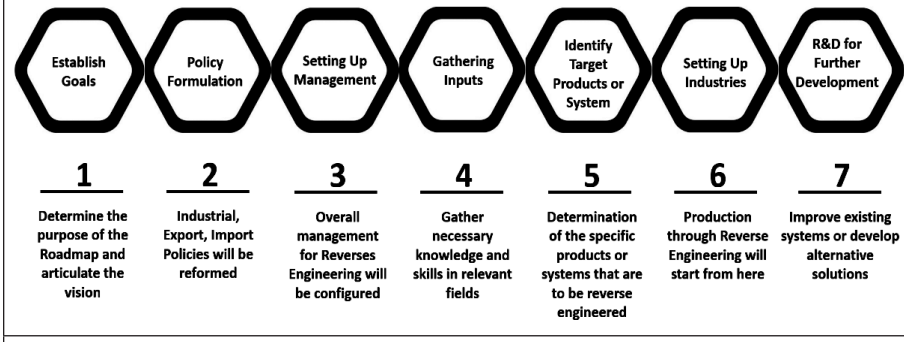
Step 4: Gathering Inputs. At this stage, it is imperative to get familiarized with the Intellectual Property Laws and Regulations in Bangladesh and also the rules and regulations of WIPO and WTO. It is also important to gather the necessary knowledge and skills in relevant fields such as engineering, computer science, and design. This is required to understand the technical aspects of the products or systems intended to be reverse-engineered. Cooperation between MIST and army-run defence industries are prerequisite for this.

Step 5: Identify Target Products or Systems. Determination of the specific products or systems that are to be reverse-engineered will be done at this stage. Factors such as demand, technical complexity, and potential benefits should be considered. This should be done by an Executive Committee at the AFD level.

Step 6: Setting Up Industries and Related Facilities. This will be the most time-consuming step. The flow of funds will be instrumental. Existing Reverse Engineering facilities in different defence industries may be strengthened and equipped for faster production.

Step 7: R&D for further Development of the Product. Now it is time to utilize the information and insights gained from the Reverse Engineering process to create innovative products, improve existing systems, or develop alternative solutions. R&D is an integral part of product management. Since technology changes rapidly, continuous R&D is important to modify the product to satisfy the needs.

Figure 3: Proposed Roadmap for Reverse Engineering



Source: Author's construct

Recommendations

After a comprehensive study, the following recommendations are submitted:

- Considering the technological intricacies, medium category and moderately advanced military arms, equipment, and vehicles may be produced through Reverse Engineering by the army-run defence industries within a time frame of 4-5 years. At the same time, effort should be made to produce high-end and technically advanced military products through TOT and JV. Low-end military products may be produced with native designs.

- AHQ Industrial Cell may standardize and categorize the existing equipment list of the Bangladesh Army like high-end and technically advanced military products, medium category and moderately advanced military arms, equipment, and vehicles and finally low-end military products like personal gear.
- A separate directorate named Defence Hardware Directorate (DHD) may be formed at the AFD level which will act as a link between DSO and different military-run organizations, academic institutions, industries and heavy workshops.
- Defence Science Organization (DSO), the apex R&D organization at the ministerial level, may be reactivated to unite the defence production capabilities and to derive technology from the private sectors.

Conclusion

The defence production projects are inherently costly and sophisticated in terms of technology. These usually take a long and unreliable gestation period for expensive R&D. Even technologically advanced and economically strong countries alone can rarely afford to develop and set up the full range of defence industries. Therefore, there is a sharp rise in the effort of TOT, JV, and Reverse Engineering besides indigenous production with native design. However, each method has its inherent advantages and disadvantages which were aptly discussed in the paper. The outcome says that, for Bangladesh, there is no single method that fits all the products in the wish list. Rather, the Bangladesh Army should start by 'mimicking' through Reverse Engineering and then switch to 'making' at the appropriate time.

This paper studied the feasibility of Reverse Engineering in Bangladesh from four different agles: Legal, Economic, Infrastructural and Technological. The legal aspect is germane to Reverse Engineering. For a country like Bangladesh, result of omission or negligence to any international rules and regulations may be catastrophic. However, careful study of patent law

and above all prudence in item selection can avoid the intricacies of legal aspects. There is a big debate about whether defence industries need to be economically rewarding or not. This study shows that, for the Bangladesh Army it has to be economically viable and it was in the cases of all reverse-engineered products so far.

Bangladesh is yet to grow the full technological prowess required for Reverse Engineering in a sophisticated way. Lack of objectivity, inadequate R&D facility, and low budget contributed to inadequate technological growth. However, the Bangladesh Army owns a good number of defence industries with untapped potential. Once integrated with the military-run academic institutions like MIST and BSMRAAU, the BOF, BMTF and BDP can be the hub of Reverse Engineering for the Bangladesh Army.

References

1. Ahmed, B. G. S., (2023). Commandant, 901 Central Workshop. Interview by Lieutenant Colonel K M Mehedi Hasan. 6 July 2023.

2. Ahmed, L.C.M.S., 2014. Prospect of Indigenous Defence Industry in Bangladesh. NDC E-JOURNAL, 13(2), pp.165-184.

3. Anis, M. G. I., (2023). Chairman, Sena Kollan Sonstha. Interview by Lieutenant Colonel K M Mehedi Hasan. 11 June 2023.

4. Arefin, Sultan, 2019, Fire Support Coordination at Higher Artillery Headquarters; Analysis and Ways Forward for Delivering Operational Fire, Artillery Centre and School.

5. Directorate of Air Operations, 2014, Draft Operational Doctrine of Bangladesh Air Force, BAF Doctrinal Publication 01-00, Dhaka: Air Headquarters.

6. Directorate of Naval Plans, 2012, Maritime Doctrine of Bangladesh, Dhaka: Naval Headquarters.

7. Douglas. M. King, 1997, The Fire Support Un-Coordination Line, Fort Leavenworth, Kansas, USA.

8. Granger, Dewey A, 2000, Coordination of Future Joint Fires: Do We Need a Joint Fire Support Coordinator, Rhode Island, U.S. Naval War College.

9. Gregory, B. Schultz, 1998, Coordinating Operational Fires for the Twenty-First Century, Fort Leavenworth, Kansas, USA.

10. Extract of the Defence Policy 2018, Peoples Republic of Bangladesh.

11. Hossain, B. G. M. M., (2023). Director Budget, Bangladesh Army. Interview by Lieutenant Colonel K M Mehedi Hasan. 27 April 2023.

12. Islam, M, A., 2010. Indigenization: a strategy for defence industrialization in Bangladesh. National Defence College, Dhaka, Bangladesh.

13. Islam, Md. Tariqul, 2022, Army Level Coordination Centre for Operational Fires: An Approach to Provide Operational Fires at Joint Operational Environment, IRP, Artillery Centre and School.

14. Jabed, Shahriar Chowdhury, 2020, Revisiting Doctrinal Fundamentals of Operational Fires for Continuing Validity, Armed Forces War Course-2020, National Defence College.

15. Jafarieh, H., 2001. Technology transfer to developing countries: a quantitative approach. University of Salford (United Kingdom).

16. Janic, M., 2018, Operation Leyte - Operational Fires, Security and Defence Quarterly, 18 (1), pp. 16-25.

17. Kurç, Ç. and Neuman, S.G., 2017. Defence industries in the 21st century: a comparative analysis. Defence Studies, 17(3), pp.219-227.

18. Langley, M. E., 1999, Operational Fires on the Urban Battlefield: An Underdeveloped Concept, Newport, Naval War College.

19. Misra, SN (2012). Impact of defence offsets on military industry capability and self-reliance. KW Publishers Pvt Ltd.

20. Naser, B. G. M. A., (2023). Security Analyst. Interview by Lieutenant Colonel K M Mehedi Hasan. 6 April 2023.

21. Noman, M. S. S., 2020. Requirement driven approach: Road map for self-reliance thorough defence industries for Bangladesh Army. National Defence College, Dhaka, Bangladesh.

22. Patents And Designs Rules, 1933. Notification No. A197, dated the 2nd of February 1933.

23. Rahman, M. G. A. K. M. Z., (2023). Executive Chairman, Bangladesh Export Processing Zones Authority. Interview by Lieutenant Colonel K M Mehedi Hasan. 25 May 2023.

24. Rasel, M. M., 2022. Defence industries in Bangladesh: Present state, foreseeable capability and steps needed for development to meet the requirements during war. National Defence College, Dhaka, Bangladesh.

25. Salehin, M. G. M. J., (2023). Engineer in Chief, Bangladesh Army. Interview by Lieutenant Colonel K M Mehedi Hasan. 11 June 2023.

26. Todd, D., 2018. Defence industries: A global perspective. Routledge.

27. Wang, W., 2010. Reverse engineering: Technology of reinvention. Crc Press. Bellevue, Washington.

Author

Colonel K M Mehedi Hasan, afwc, psc was commissioned on 07 June 2000 with 42nd Bangladesh Military Academy Long Course in the Corps of Engineers. He served in different Engineer Battalions at various regimental appointments. He commanded an Engineer Construction Battalion and a Division Engineer Battalion. In staff appointment, he served as a Brigade Major of a Composite Brigade. He served as an Instructor Class 'C' at the Engineers Centre and School of Military Engineering (ECSME). He was Platoon Commander and Term Commander at Bangladesh Military Academy. Presently, he is serving as Colonel Staff, 33 Infantry Division Colonel Mehedi is a graduate of Civil Engineer from the Military Institute of Science and Technology (MIST). He is also a graduate of Defence Services Command and Staff College, Mirpur. He attended a second staff course in Sri Lanka. He has three master degrees in his credentials. Colonel Mehedi had his tour of duty in the United Nations Mission in Liberia. He commanded a Demining Contingent in Kuwait under Operation Kuwait Punargatan (OKP). Colonel Mehedi has a publication in Bangladesh Army journal titled 'Cascading the Philosophy of Mission Command (Auftragstaktik) from the Prussian Army Down to the Bangladesh Army: Exploring the Feasibility'. He is happily married to Kamrun Nahar Mithun and blessed with one son and a daughter.

NDC JOURNAL
Security Through Knowledge

QUEST FOR A SUSTAINABLE KNOWLEDGE MANAGEMENT ARCHITECTURE: OPTIMISING EXISTING RESEARCH-BASED KNOWLEDGE OF BANGLADESH ARMED FORCES

Lieutenant Colonel Quzi Md Nahidul Islam, SUP, afwc, psc, Infantry

Introduction

The quest for a sustainable knowledge management (KM) architecture is of paramount importance in today's organisations, which often find themselves "drowning in information but starved for knowledge" (Naisbitt, 1984, p. 17, cited by Bartczak, 2002). KM has its roots in ancient philosophy and has evolved to encompass the historical viewpoint of managing knowledge effectively. KM methodologies have expanded beyond for-profit organisations to include non-profit entities, such as government and non-government organisations, recognising its pivotal role in achieving organisational success (Hislop, 2013). Effective KM involves acquiring, retaining, disseminating, and applying knowledge, enabling organisations to maintain a competitive edge and meet stakeholder demands (De Long & Fahey, 2000). While KM is relatively new in the Armed Forces, its significance steadily increases. Implementing KM processes and systems in military organisations requires understanding various factors, including organisational changes, cultural dynamics, leadership styles, technological advancements, evaluation of KM initiatives, and available resources (Holsapple & Joshi, 2002).

The Bangladesh Armed Forces (BDAF), a source of national pride, generates substantial research-based knowledge (RBK) through the participation of officers in various courses and training programs. However, the BDAF lacks a sustainable KM infrastructure to effectively utilise this RBK, resulting in knowledge redundancy, data loss, and difficulties in sharing

and retrieving information. To address this gap, a tailored KM architecture is needed to optimise the utilisation of the BDAF's RBK and foster innovation. This study aims to comprehensively analyse a sustainable KM architecture, including its elements, benefits and challenges, and propose its implementation within the BDAF. By developing an effective KM architecture, the BDAF can leverage its vast and diverse RBK, improve organisational performance, and promote innovation. The study will also explore the barriers to implementing KM in the BDAF, such as limited resources, technology, and understanding of KM concepts, and propose solutions to overcome these challenges. Incorporating web technologies in the KM architecture will simplify the application of KM practices and enable efficient sharing, storage, and retrieval of RBK (Hislop, 2013; Akeriwa et al., 2014). By optimising the utilisation of RBK, the BDAF can enhance its organisational outcomes and contribute to innovation.

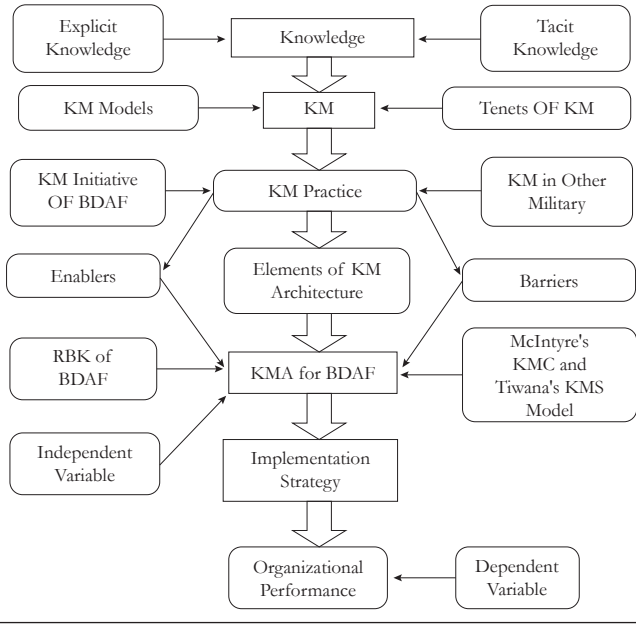
Literature Review

For this research, several relevant literatures have been reviewed to get a clear insight into this topic. The oldest proponent of the KM system, Karl Martin Wiig's cohesive and practical outlook on KM emphasises the organisation of knowledge to make it valuable (Dalkir, 2011). Zhang (2013) highlights the distinction between tacit and explicit knowledge, with explicit knowledge being more suitable for KM methods. Military KM focuses on the need-to-know basis and leverages knowledge within the military, promoting cooperation to achieve mission goals (Ismail et al., 2011). The Nonaka model emphasises converting tacit knowledge into explicit knowledge, leading to innovation (McIntyre et al., 2003). Effective KM systems facilitate generating, disseminating, and combining knowledge across different domains. The evolution of KM is viewed as an increasingly important discipline that promotes creating, sharing, and leveraging organisational knowledge (Fernandez et al., 2004). KM facilitates creating and using knowledge for increased innovation and value, profoundly influencing organisational excellence. However, no KM architecture exists for BDAF, and no research has been conducted. Therefore, this research will be the first of its kind.

Methodology

The research methodology for developing a sustainable KM architecture for BDAF involves an exploratory approach with a causal relationship. A mixed-method approach, combining quantitative and qualitative data, was used to analyse the linkage among organisational performance, human capital capacity, KM architecture, and sustainable KM. Data were collected from primary and secondary sources, including Key Informant Interviews (KII), observations, and Focus Group Discussions (FGD). The significance of this research lies in its potential to benefit the BDAF, policymakers, and researchers by providing insights into implementing KM practices, improving organisational performance and reducing knowledge redundancy within the BDAF. The research aims to contribute new knowledge in the field of KM, particularly in developing a sustainable KM architecture that can optimise existing RBK. The analytical framework (figure 1) of the research is appended below:

Figure 1: Analytical Framework



Source: Researcher's construct

Result

Knowledge and Its Categories

The concept of "knowledge" has been debated by philosophers since ancient times. According to Tiwana (2002), knowledge refers to relevant information accessible in the right place, at the right time, and in the proper framework. On the other hand, Fernandez, Gonzalez, and Sabherwal (2004) distinguish knowledge from data and information by stating that knowledge consists of facts and observations, while data is raw numbers without context or purpose. Information, in turn, is processed data that reveals hidden trends and patterns.

Nonaka (1994) identified two types of knowledge in organisations: tacit and explicit. Tacit knowledge is subjective, ingrained in people's minds, and related to experience and ability. It is difficult to record or articulate, consisting of intelligence, judgement, values, and assumptions. On the other hand, explicit knowledge is easily expressed, codified, and transferred through language or media. It is formalised, structured, and easily communicated, making it accessible through information systems and repositories. Several other writers believe that tacit and explicit knowledge are complementary, where 30% of explicit knowledge is articulated while 70% of tacit knowledge is not articulated (figure 2). This makes explicit knowledge more suitable to be managed with KM methods.

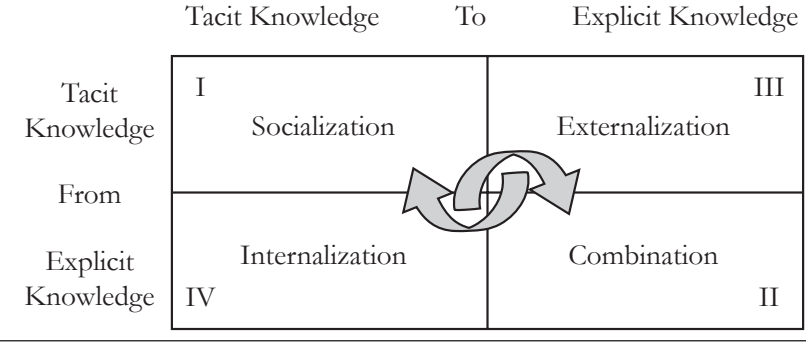
Figure 2: Tacit/Explicit Knowledge Dimensions

Source: Putter, A.P., 2018

KM and KM Models

- **KM.** KM refers to systematic activities to enhance an organisation's knowledge-related capabilities. It includes creating, sharing, using, and managing knowledge to foster improved performance and innovation.
- **Nonaka's SECI Model.** Nonaka's SECI model is a well-known KM model that shows how knowledge is made. The SECI model says that knowledge is made in a spiral, moving from implicit to explicit knowledge and then back to implicit knowledge. It involves four stages, as shown in figure 3:

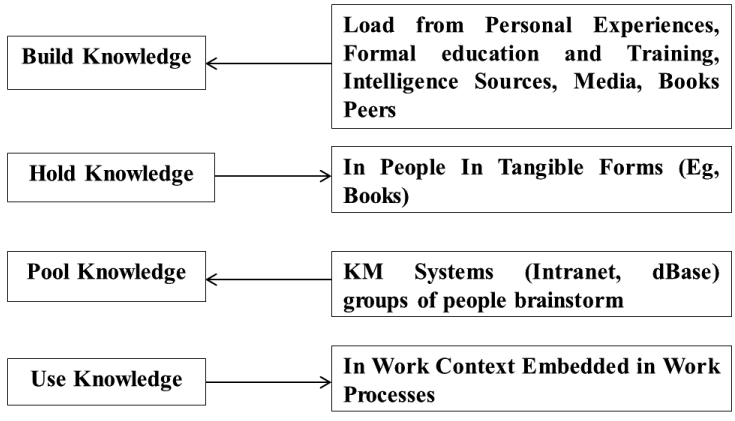
Figure 3: Model of Knowledge Creation



Source: Nonaka (1994)

- **Wiig's Model.** WIIG identifies the primary objective of KM as "to make the organisation intelligent acting by facilitating the creation, accumulation, deployment, and use of high-quality knowledge." The four essential steps of the WIIG model are shown in the figure 4.

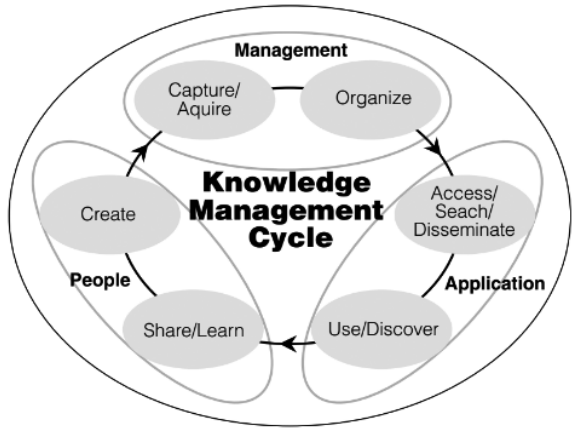
Figure 4: WIIG model



Source: WIIG (1993)

- **McIntyre KMC.** The KMC refers to how an organisation transforms information into knowledge. Figure 5 model shows how knowledge-transformation processes are set up in a KM environment. The KMC, recommended by McIntyre, has six phases, each with a unique orientation in different organisational departments: people, management, and application.

Figure 5: KMC

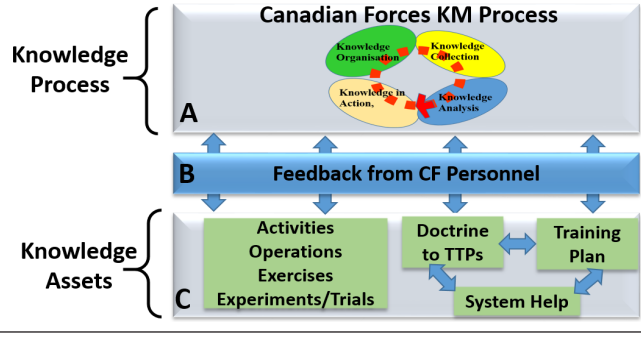


Source: McIntyre, Gauvin and Waruszynski (2003)

Best Practices of KM Theories and Models in Military

The US Military utilises the Army Knowledge Online system, which promotes knowledge-sharing and collaboration among soldiers. The Australian Defence Force follows the SECI model to capture and share knowledge, emphasising a learning culture. The Singapore Armed Forces employs the Integrated KM System to capture, store, and share knowledge, including lessons learned. The Canadian Forces (CF) use the Canadian KMS within the Land Force Command and Control Information Systems (LFC2IS) to support decision-making and continuous learning (figure 6). The Indian Armed Forces utilises a KMS based on the DIKW model, emphasising knowledge sharing and collaboration.

Figure 6: LFC2IS



Source: Champoux, P., Costello, M.J. and Bourget, S., (2005)

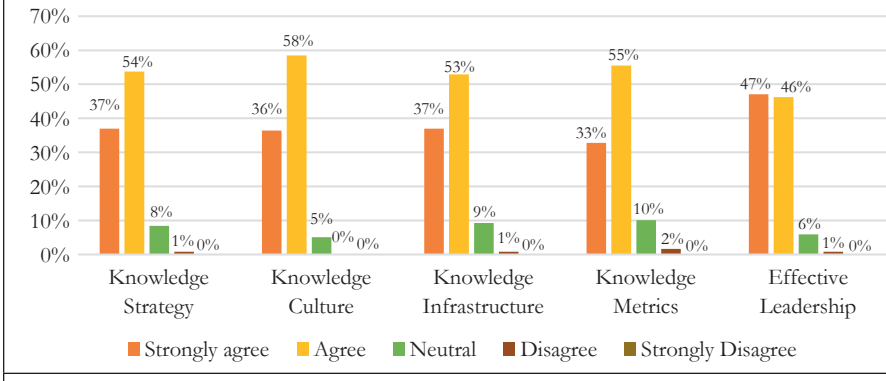
The Current State of KM of RBK in BDAF

The BDAF currently lacks a separate strategy for KM of RBK. KM functions within the armed forces are primarily planned, coordinated, and executed by the Services Headquarters, with some involvement from formations and other institutions. However, there are several impediments to KM within the BDAF. These include the absence of a KM framework, inadequate mechanisms for capturing and disseminating research results, the lack of networks and platforms for sharing RBK, and a limited knowledge-sharing culture.

Critical Elements of a Sustainable KM Architecture

Survey results validate the importance of five critical elements for a sustainable KM architecture: knowledge strategy, knowledge culture, knowledge infrastructure, knowledge metrics, and effective leadership (chart 1). To address the KM of RBK, the BDAF should develop a distinct knowledge strategy aligned with organisational goals, foster a knowledge-sharing culture, establish a robust knowledge infrastructure, implement knowledge metrics for evaluation, and ensure strong leadership support. By implementing these measures, the BDAF can effectively manage and leverage its intellectual resources, leading to improved organisational performance and the creation of new knowledge.

Chart 1: Responders' Outlook on Key Elements of KM Architecture



Source: Survey

KM Enablers in Military

Organisations widely recognise KM as their most valuable asset. The development of technology has dramatically influenced KM. KM involves formal, informal and complex methods to facilitate knowledge distribution and growth, often with the support of technology. However, there are enablers of KM found in various literature (table 1) that need to be studied for better management of RBK through KM architecture.

Table 1: List of Enablers	
Author	**Enablers**
Arthur Anderson (1996) & APQC (1996 & 1999)	Leadership, corporate culture and IT infrastructure measures for assessing performance
Earl (1997)	Information Technology, HR & organization culture
Skyme & Amidon (1997)	Knowledge leadership includes Vision, knowledge-creating and sharing culture. Continuous learning, Technology infrastructure
Holsapple & Joshi (1997)	Managers, Resources such as technology and infrastructure and working environment
Liebowitz (1998)	Strategy adopted by senior management, KM infrastructure, knowledge ontology and repositories, KM systems and tools, incentives, for knowledge sharing, and collaborating/cooperating culture
Davenport Probst (2002)	Leadership, training, measure performance well, defined policy, knowledge acquisition & sharing, IT infrastructure
Mathi (2004)	Culture, systemic process, Knowledge Management framework and Technological infrastructure
Source: Nagendra, A. and Morappakkam, S., 2016	

The above literature and FGD, suggest that BDAF should incorporate several key elements for developing a sustainable KM architecture. These elements include improved accessibility to information, enhanced knowledge sharing mechanisms, more effective knowledge creation processes, optimized decision-making capabilities, seamless knowledge integration, robust knowledge preservation systems and strengthened collaborative frameworks.

Potential Challenges in Implementing KM Architecture for BDAF

Establishing a resilient KM framework is crucial for organisations as it enables knowledge generation, dissemination, and preservation, leading to improved organisational performance and the creation of new knowledge. However, a study conducted by Nagendra and Morappakkam (2016) reveals several barriers or challenges identified in various literature that hinder the effective implementation of KM (table 2). The study also explores the origins of these challenges.

Table 2: List of Barriers

Author (Year)	Barriers Focus	Area
Ladd and Ward (2002) and Hansen and Avital (2005)	Competitiveness within an organization	Leadership, Individual
Bartol and Seivastava (2002) and Hexmoor et al (2006)	Knowledge is power, and perception resulting in a lack of sharing has been noticed	Organization Culture
Riege (2005)	Insecurity or ignorance about the value of one's knowledge & a high level of organizational stratification Individual	Organizational Structure
Goman (2002)	Unconscious competence, as referred to it; zero tolerance; and a low readiness to accept new ideas	Leadership organization Culture
Ladd and Ward (2002)	Bureaucracy	Leadership

Table 2: List of Barriers		
Author (Year)	**Barriers Focus**	**Area**
Stevens, (2002) Skyrme (2002)	Employee and employer goal divergence; functional silos	Leadership organization Culture
Figallo and Rhine (2002)	Lack of top management support	Leadership
Carr et al (2003) and Hexmoor et al (2006)	Security requirements	organization Culture
French and Michae145 (2003) and Riege (2005)	Power struggle or control of the use of the knowledge or information	Leadership organization Culture
Kellogg (2003)	Closed information environment (US Defence Department) hierarchical Organizational structures	Organizational Structure
Davidson and Voss (2002); Figallo an Rhine (2002)	Lack of training in both technical and interpersonal skills	Leadership
Skyrme (2002): Stoddart (2001)	Lack of tools or inadequate systems, poor information quality	Technology
Lunney (2002); Stoddart (2001)	Lack of time and resources	Organization Climate
Source: Nagendra, A. and Morappakkam, S., 2016		

It is important to note, though, that not all of these barriers apply to the specific context of the BDAF. Therefore, this discussion focuses on the challenges of implementing KM for RBK as revealed through surveys, FDG, and interviews. These challenges include integrating existing systems, lack of awareness and training, technology and infrastructure limitations,

limited resources, data quality and availability, organisational complexity, information security, and cultural barriers. The survey results indicate that respondents acknowledge the difficulties associated with these challenges, with varying percentages ranging from 81% to 92%. Overcoming these challenges requires addressing the needs of stakeholders, conducting regular training and awareness programs, allocating resources effectively, prioritising software updates, validating RBK assets, implementing strict information security protocols, and addressing cultural challenges within the organisation.

KM Model Considered for BDAF KM Architecture

Based on the study, KMC by McIntyre (2003) is found to be best suited for the management of RBK of BDAF. This has three domains with six phases, which focus on different aspects of managing knowledge within an organisation. The first phase is centred on people and emphasises learning, sharing, and collaboration. This phase belongs to the cycle's domain of people. However, individuals could be considered knowledge producers and consumers. Their contribution is optimal within the parameters of the KMC's people component. This stage lays the groundwork for the second stage, which focuses on creating knowledge. To develop valuable knowledge, individuals must effectively share and collaborate. The more effectively knowledge is shared, the more valuable the repository created.

The focus shifts to the management domain in the third phase of the KMC. This phase entails collecting and storing newly generated knowledge (RBK) in a central repository. Technological tools for managing content and documents, including acquiring explicit and tacit knowledge, have been developed to support this endeavour. After acquiring the inside, it must be organised for easier accessibility. This organisational process takes place during stage four of the KMC.

The fifth stage, also known as the application domain, aims to make this RBK accessible to employees. Individuals can use this knowledge to solve

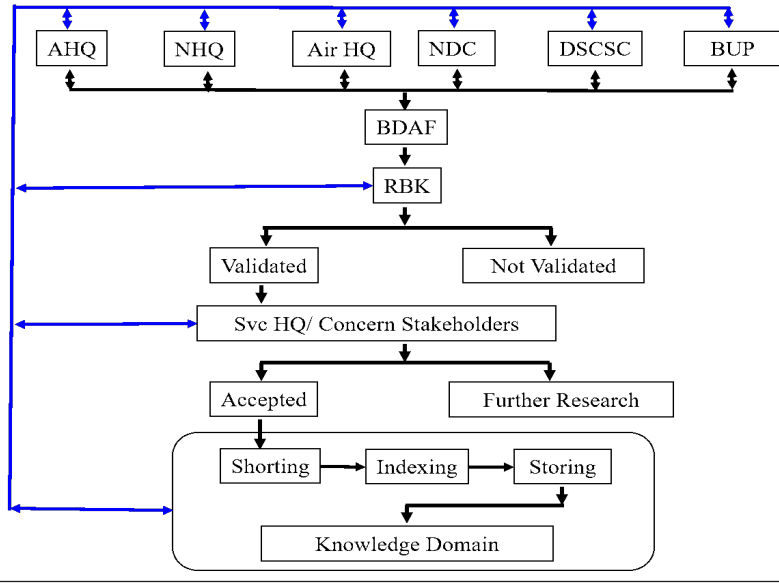
problems, which is the ultimate objective of the final phase: use and discovery. Indeed, KM offers numerous opportunities to acquire and share data in repositories, allowing organisations to capitalise on their collective knowledge resources.

This KMC raises the question. How do we create a knowledge repository of RBK? What practical and sustainable KM architecture would facilitate improved knowledge management of BDAF contemporary research works? Additionally, how does BDAF implement the KMC model to generate new knowledge? The KMC model has already been implemented in the Canadian Forces, NATO, and the US Army. Based on the study, for BDAF, the KMC model can be enhanced by integrating a knowledge management system (KMS). This integration will assist users in sharing and utilising the knowledge repository of RBK to generate new knowledge.

Knowledge Repository of RBK of BDAF

The BDAF conducts many research studies annually, all of which contribute to forming new bodies of information. However, Abedin (2023) opined that the RBK generated by individual or group members of the BDAF typically remains within the specific service headquarters or institutions and is not shared or disseminated adequately. Therefore, it is essential for all stakeholders to actively participate in sharing their knowledge within a dedicated knowledge domain to address this challenge effectively and ensure the effective management of this valuable knowledge, as stated by Ridwanur (2023). This sharing of knowledge can be facilitated by creating a knowledge repository. Figure 8 suggests the flow of RBK within the BDAF to create a knowledge repository in the knowledge domain for improved knowledge sharing and utilisation throughout the organisation.

Figure 7: Flow of RBK within BDAF

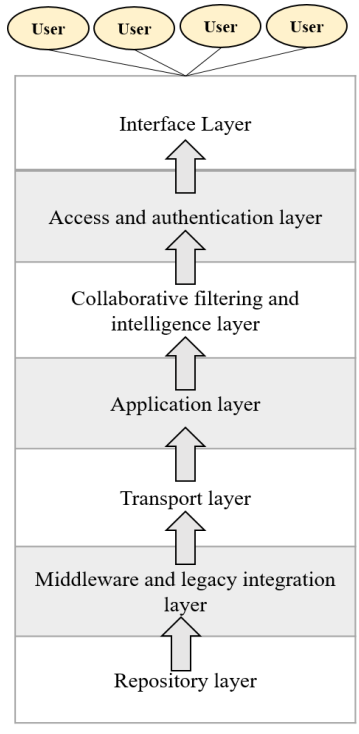


Source: Researcher's construct

KM System Architecture

Once knowledge is created, it is significant to disseminate the knowledge to the members of the organisation through the appropriate system or tools. Tiwana (2002) attempted to suggest a general KMS architecture (figure 8). He indicates that KMS architecture should consist of seven essential components to share and use knowledge for creating new knowledge. In the KMS, the repository layer provides a central repository for storing and managing knowledge assets. The middleware and legacy integration layer enables integration with other enterprise systems. The transport layer manages data transfer between KMS components. The application layer includes core functionalities like document management and search. The collaborative filtering and intelligence layer facilitates knowledge sharing using machine learning techniques. The access and authentication layer ensures secure access to the KMS. The interface layer serves as the user interface for interacting with the KMS.

Figure 8: KMS Architecture

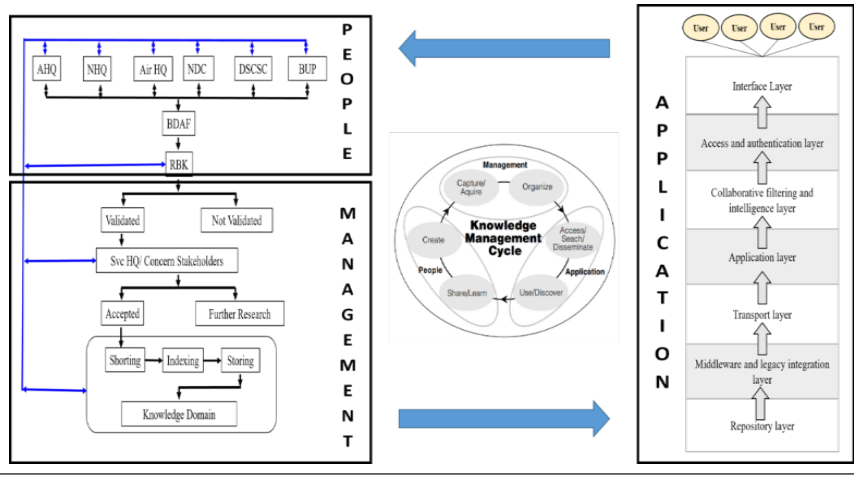


Source: Tiwana (2002)

Sustainable KM Architecture for BDAF

Based on the discussion, two crucial factors are considered: the efficient management of RBK within the BDAF through the KMC and the dissemination of this RBK through a KMS to foster the sharing and production of new knowledge. Both of these factors are taken into account. The comprehensive KM mechanism and the process of sharing knowledge through a sustainable KM architecture are explained in detail in Figure 9. Combining KMC by S. G. McIntyre and KMS by Tiwana, this KM architecture is constructed to manage and share the RBK. This KM architecture comprises three separate phases: the creation of knowledge(people), the management of that knowledge, and the dissemination (application) of that knowledge.

Figure 9: Sustainable KM Architecture for BDAF

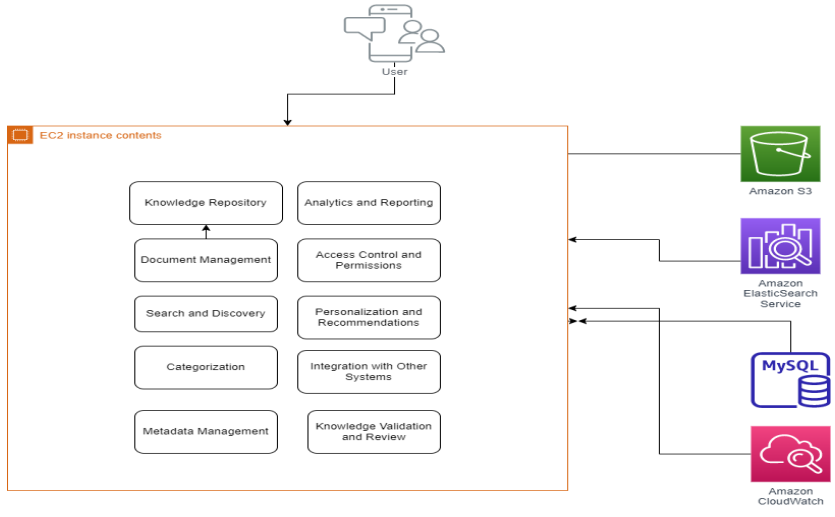


Source: Constructed Based on the KMC by S. G. McIntyre and KMS by Tiwana

Creating RBK within the BDAF begins with its members conducting research, which is then thoroughly examined and filtered by competent authorities. This will mark the beginning of the first phase. In the second phase, the RBK is effectively managed by the KMC, ensuring that it is organised and utilised correctly. The final phase of the process involves the RBK being distributed to the participants of the BDAF, thus completing the cycle in a closed-loop fashion. The KMS acts as an effective facilitator throughout the process.

The model has undergone additional development with software expertise (Moinur, 2023) to enable its implementation within the BDAF. This workable model (figure 10) has three primary considerations:

Figure 10: High-Level Diagram of the System



Source: Constructed Based on Interview (Moinur, 2023)

- **System Overview.** The system has several components to create an efficient and secure Knowledge Management Architecture (KMA). The central database serves as a repository for knowledge and information, allowing for easy organisation and retrieval. Artificial Intelligence (AI) is implemented through Natural Language Processing (NLP) techniques such as Topic Modeling and Named Entity Recognition (NER), enabling keyword and phrase matching. A web server hosts the KMA application and handles user requests, while a user interface allows users to interact with the system through a web browser or mobile application. Security measures are in place to ensure that only authorised users have access to the KMA and its data.

- **Functional Requirements.** The functional requirements of a KMA include several components. The knowledge repository acts as the central database for storing various knowledge assets. Document management organises and controls the storage of documents within the repository. Content creation and editing enable users to contribute and collaborate on knowledge content. Search and discovery functionalities allow users to find relevant content quickly. Categorisation systems ensure logical

navigation. Metadata management captures and manages attributes about knowledge content. User profiles capture users' expertise, while collaboration tools promote engagement. Knowledge validation procedures ensure accuracy before sharing. Analytics and reporting tools track usage and effectiveness. Access control and permissions restrict access based on roles. Integration with other systems facilitates knowledge sharing. Virtual assistants and chatbots assist users. Personalisation and recommendations utilise algorithms. The system should allow document upload and use AI for categorisation.

- **Non-Functional Requirements.** The non-functional elements of a KMA include several aspects. Performance requirements involve supporting concurrent users and maintaining fast response times for searches and article retrieval. Security requirements include data encryption during transmission and storage and role-based access control for data confidentiality. Usability requirements focus on an intuitive and easy-to-navigate user interface and mobile responsiveness for access from different devices. Scalability requirements involve designing the system to handle increasing data and user load. Reliability requirements include regular data backups and a disaster recovery plan. Compatibility requirements include support for popular web browsers and operating systems.

Implementation Strategy of KM Architecture

The implementation strategy for a knowledge management architecture can change depending on the goals that it seeks to achieve. However, for BDAF, the implementation process can be guided by the following steps and considerations (FGD):

- **Evaluate the KM Architecture.** The suggestive model of KM architecture is to be implemented as a pilot project in BDAF with a provision of reviewing it each after 12 months.

- **Formulate Policy and Objectives.** Define the goals of the KM architecture with the overall objectives and strategies. These objectives need to be SMART, which stands for specific, measurable, attainable, relevant, and time-bound. Rashed (2023) opined that an appropriate law governing the KM architecture and research activities in Bangladesh should be passed in Parliament, giving policy guidelines to all concerned.
- **Acquire the Support of the Leadership.** Armed Forces Division should involve senior leadership, as they are the ones who will be able to direct the implementation of the KM architecture and assign the necessary resources.
- **Construct a Roadmap.** Create a road map that outlines the implementation strategy, including significant milestones, projects, and dependencies, and then follow that road map.
- **Construct Organisational Structure.** A separate organisation may be established at the tri-service level with adequate authority to streamline the KM architecture and regulate research activities within BDAF. This organisation should be led by a senior officer (Major General/ equivalent and above) to bring synergy into the research activities (Abedin, 2023).
- **Monitor and Assess the Situation.** Maintain a continuous evaluation of the effectiveness of the KM architecture and the tracking and collection of feedback on the implementation's progress. In this regard, BUP should exert more quality and regulatory control over various training institutions of BDAF for research activities only (Rashed, 2023).
- **Promote a Culture of Sharing Knowledge.** Develop a culture that values and actively promotes working together and sharing information.

Recommendations

Suggested recommendations are illustrated below:

- A separate organisation may be established at the tri-service level with adequate authority to streamline the KM architecture and regulate research activities within BDAF. This organisation may be led by a senior officer (Major General/equivalent and above) to bring synergy into the research activities.
- Existing training and doctrine divisions of different services are to be brought under the newly suggested structure for the issue of KM architecture and research activities only.
- A suggestive model of KM architecture is explained to be implemented as a pilot project in BDAF with a provision of reviewing it each after 12 months.
- BUP may incorporate a regulating body for KM, which should exert more quality and control over various training institutions of BDAF for research activities only.

Conclusion

KM has its roots in the early stages of Ancient Greek philosophy and epistemology. This concept has evolved, expanding to include a historical perspective on KM. Today, KM methodologies are increasingly adopted, and their influence extends beyond for-profit organisations to include government and non-government agencies. Organisations must use KM well to keep their competitive edge and meet the needs of their stakeholders. Even though KM is still a reasonably new idea in the Armed Forces, its importance is slowly being understood. However, there is currently no sustainable KM infrastructure to utilise RBK effectively. Each year, the BDAF conducts research that generates substantial amounts of RBK in numerous fields. The lack of this results in the loss of valuable information, making it difficult to share, store, and retrieve data, ultimately

leading to the underutilisation of RBK. The absence of an effective KM infrastructure also results in knowledge redundancy and retrieval issues. It is imperative to close this gap by developing a KM infrastructure tailored to meet BDAF's requirements, considering the complexities of existing RBK and facilitating their productive utilisation.

There are two types of knowledge: tacit and explicit. Tacit knowledge is held in the minds of individuals, is personal and context-specific, and is difficult to formalise and transmit. On the other hand, explicit knowledge is easily expressed, articulated, codified, and transferred between individuals or systems, making it simple to disseminate and comprehend. RBK, being the explicit knowledge, can be well managed through KM architecture to enhance an organisation's knowledge-related capabilities by creating, sharing, applying, and managing knowledge. Over 90% of respondents believe optimising RBK assets can improve BDAF's information access and facilitate knowledge sharing. Sustainable KM influences organisational performance positively and moderates the relationship between human capital knowledge and organisational performance. Consequently, integrating sustainable KM into all organisational processes can enhance the knowledge and performance of human capital. The current void in BDAF's KM architecture necessitates immediate attention to utilising RBK efficiently.

The KMC refers to the process by which an organisation transforms information into knowledge, and KM System disseminates the knowledge to the organisation's members through the appropriate system. A new architecture combining McIntyre (2003) and Tiwana (2002) can be utilised to manage RBK and prevent duplication of efforts effectively. Taking these two models into account, a workable model has been prepared. The model incorporates information and communication technology, including AI, to provide BDAF members access to the RBK of previously conducted research. The implementation strategy emphasises aligning KM objectives with desired outcomes, conducting a comprehensive evaluation of the current situation, formulating SMART objectives, acquiring leadership support, developing a flexible road map, establishing an organisational

structure and processes, executing and communicating the plan, monitoring and assessing progress, and promoting a culture of knowledge sharing. The KM architecture enables efficient RBK management by providing features such as user authentication, document management, content creation, and search functionality.

References

1. Air Commodore Md Abu Rayhan, GUP, BUP, ndc, psc, GD(P), Director of Air Training, Air Headquarters, Interview 03 August 2023.
2. Akeriwa, T. O., Penzhorn, C., & Holmner, M. A. (2014). Utilisation of Web 2.0 technologies for knowledge sharing among academics in a developing country. SA Journal of Information Management, 16(1), 1-11.
3. Brigadier General Muhammad Ashrafuzzam Siddiqui, BSP, SUP, ndc, psc, Director Military Training Directorate, AHQ, Interview 11 June 2023.
4. Brigadier General Hussain Muhammad Masihur Rahman, SGP, SPP, ndc, afwc, psc, Director General Operations and Plan Directorate, AFD, Interview 11 June 2023.
5. Brigadier General Md Mofizul Islam Rashed, afwc, psc, Commander, 52 Infantry Brigade, Interview 11 August 2023.
6. Bartczak, S. (2002). Knowledge Management in the Military Context: An Overview. Journal of Knowledge Management Practice, 3(1), 1–13.
7. Champoux, P., Costello, M.J. and Bourget, S., 2005. The Canadian knowledge management system (KMS) within the land force command and control information systems (LFC2IS). In 10th International Command and Control Research and Technology Symposium (ICCRTS) (pp. 1-13).
8. Commodore Mohammad Joynal Abedin (ND), NGP, NDC, AFWC, PSC, PHD, BN (Director Naval Training), NHQ, Interview 11 June 2023.
9. Dalkir, K. (2011). Knowledge Management in Theory and Practice, 2nd Ed., Cambridge, MA: Massachusetts Institute of Technology.

10. De Long, D. W., & Fahey, L. (2000). Diagnosing cultural barriers to knowledge management. Academy of Management Executive, 14(4), 113–127.

11. Fernandez, Irma Becerra., Gonzalez, Avelino., and Sabherwal, Rajiv. (2004). Knowledge management: Challenges, solutions, and technologies. New Jersey: Prentice Hall.

12. Hislop, D. (2013). Knowledge management in organisations: A critical introduction. Oxford University Press.

13. Holsapple, C. W., & Joshi, K. D. (2002). Organisational knowledge resources. Decision Support Systems, 33(1), 3-15.

14. Ismail, M. and Abdullah, R.Y.R., 2011. Perception of knowledge creation, knowledge management processes, technology and application in military organisations. Malaysian Journal of Library & Information Science, 16(1), pp.73-85.

15. Major General A S M Ridwanur Rahman, awc, afwc, psc, G, Comdt, BIPSOT, Interview 30 July 2023.

16. McIntyre, S.G., Gauvin, M. and Waruszynski, B., 2003. Knowledge management in the military context.

17. Moinur Hosain Chaudary, Software Engineer, CEO, Soft Wind Tech, Interview 16 August 2023.

18. Naisbitt, J., (1982). Megatrends. New York: WarnerBooks.

19. Nagendra, A. and Morappakkam, S., 2016. Knowledge management enablers and barriers in the army: an interpretive structural modelling approach. Indian Journal of Science and Technology, 9(45), pp.1-12.

20. Nonaka, I. and Takeuchi, H., 1995. The Knowledge-Creating. New York, 304.

21. Putter, A.P., (2018). Knowledge Management for the South African Department of Defence (Doctoral dissertation, Stellenbosch: Stellenbosch University).

22. Tiwana, A., (2002). The knowledge management toolkit: Orchestrating IT, strategy, and knowledge platforms. Pearson Education India.

23. Wiig, Karl M. (1993). Knowledge management foundations: Thinking about thinking – how people and organisations create, represent, and use knowledge. Texas: Schema Press.

24. Zhang, H. (2013). Knowledge of integrated business process management for third-party logistics companies. PhD dissertation. Germany: University of Bremen.

Author

Lieutenant Colonel Quzi Md Nahidul Islam, SUP, afwc, psc, was commissioned in the Corps of Infantry on 27 December 2001 with 45th BMA Long Course. He held various appointments in several Infantry Regiments. He served as General Staff Officer Grade-3 (operations) at 69 Infantry Brigade. He also served as Instructor Class-B at the School of Infantry and Tactics and as Senior Instructor at the Bangladesh Infantry Regimental Center. Lieutenant Colonel Nahid also raised and took command of the 62 East Bengal and played a crucial role in forming the 7 Infantry Division. Besides, he has represented Bangladesh in the United Nations Mission in Liberia (UNMIL) as a Platoon Commander in BANBAT-13. He also participated in the United Nations Mission in South Sudan (UNMISS) as a senior staff officer in Movement Control (MOVCON) in the Mission Support Division. He has undergone a Special Operation Company Command Course from Sizuazuhang Military Academy, China. He graduated from the Defence Services Command and Staff College and National Defence College, Mirpur. He obtained a Master of Science in Military Studies and Social Science and Development from Bangladesh University of Professionals. He has been serving as General Staff Officer-1 at the Army Headquarters, Weapon, Equipment and Statics Directorate.

NDC JOURNAL
Security Through Knowledge

IMPACT OF 4IR TECHNOLOGY ON NAVAL WARFARE: CHALLENGES FOR BANGLADESH NAVY (BN) AND WAYS FORWARD

Commander Mahbuba Afroze, (L), afwc, psc, BN

Introduction

The impact of 4IR Technology is wide-ranging and it is going to shape the future battle field (Tangredi & Galdorisi, 2021). Navy is predominantly a technology intensive force. The technological innovation impacts naval warfare and tactics deeply; and ascendancy in technology by one ensure marked advantage over an adversary (Vincent O'Hara, 2022). 4IR Technology can offset these hindrances and can enhance the naval combat capability significantly. For this reason, the Bangladesh Navy (BN) also needs to adopt 4IR Technology to give its war fighters the edge in combat. However, it is difficult to research on all elements of 4IR Technologies like AI, robotics, Big Data, 3D Printing and IoT etc. In the context of this study, AI and Big Data are discussed only as 4IR Technologies.

4IR Technology is deeply infusing naval warfare, as such the major navies of USA, UK, France, Russia and China have already embraced 4IR Technology. India, South Korea, Singapore and some other countries are feverishly working on incorporating 4IR into a multi-domain that includes the Navy. These have significant implications for naval operations by BN. As such, Bangladesh Navy will have to adopt 4IR Technology specially AI and Big Data to suit with the contemporary naval warfare. Consequently, the question remains, what are the challenges and how best BN can adopt 4IR Technology? The possible challenges to adopt could be legacy mind set, budgetary constraint, technical challenges, human resources, industry support, cyber security and data confidentiality. However, it is not possible for BN to adopt all elements of 4IR Technology for this moment but she can adop AI and Big Data initially for enhancing the combat capability.

Research Objectives

Main Objective. The broad objective is to analyse the impact of 4IR Technology on Naval Warfare and suggest options for BN to adopt 4IR based Technology.

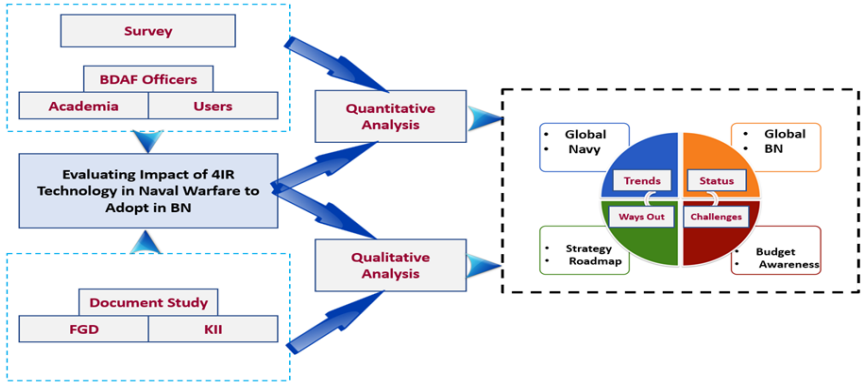
Specific Objectives

- To understand the military application of 4IR and its impact in naval warfare.
- To determine the current status of BN in terms of 4IR based technology.
- To identify the scope of upgrading for BN in adopting 4IR based technology.
- To propose a strategy for BN to adopt 4IR based technology and to formulate a pragmatic road map.

Research Methodology

The research falls within purview of 'Exploratory Research'. This was a cross sectional study focusing the causal relationship design. The research employed a mixed-method (quantitative and qualitative data) research design to explore challenges and ways out for BN to adopt 4IR Technology for the enhancement of BN warfare capability. Besides, it followed a conceptual methodology basing on multiple source of information. Surveys, Key Informant Interviews (KII), Focused Group Discussions (FGD), Case Study and content analysis have been conducted in this study. In addition to using primary data, reputable sources of secondary data have also been employed.

Figure 1: Research Methodology



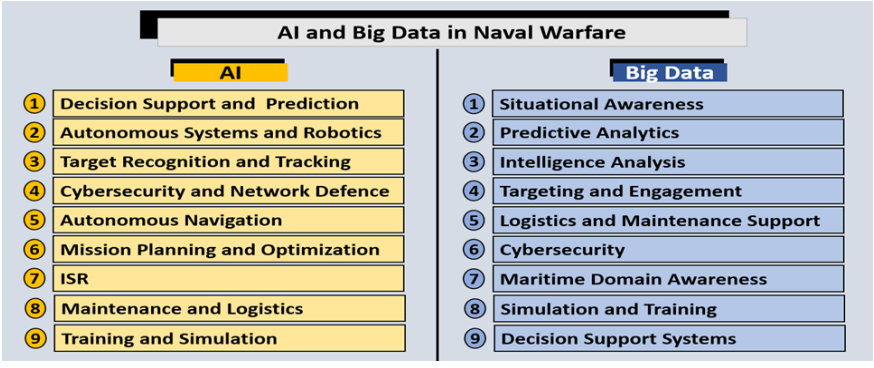
Source: Author Construct

Impact of AI and Big Data in Naval Warfare and Its Application in World Navies

Military Application of 4IR Technology. The military is actively exploring and adopting various 4IR technologies to enhance its capabilities and operations. Some of the military applications of 4IR technology include:

Impact of AI and Big Data in Naval Warfare. The utilisation of AI has gained significant importance in modern naval warfare, as it offers valuable insights and improves operational capabilities. In essence, AI offers naval forces an array of benefits including heightened situational awareness, predictive capabilities, and enhanced decision-making capabilities. It helps in target detection, selection, identification and engagement, for examples, hypersonic missile which is humanely impossible to react and defend without help of AI and Big Data. Big Data analytics has become increasingly important in contemporary naval warfare, providing valuable insights and enhancing operational capabilities. In summary, big data analytics provides naval forces with enhanced data analysis, predictive capabilities, intelligence analysis and quick decision-making.

Figure 2: AI and Big Data in Naval Warfare



Source: Author Construct

Case Studies

USA. According to recent research by Brett Vaughan (2022), US Navy is presently engaged in the active design and development of more than 1000 activities linked to AI. Within the realm of AI, US Navy places significant emphasis on the use and development of UAVs as well as naval vessels. The utilisation of swarm drones, unmanned boats, underwater drones, the X-47B prototype drone, and the Sea Hunter Anti-Submarine Warfare system are examples.

India. The Defence Advanced Research Projects Agency (DARPA) and the Defence Research and Development Organisation (DRDO) have established a working alliance to participate in AI technical pursuits. The existing inventories of AI technologies within the Indian Armed Forces comprise a range of UAVs, including the IAI Searcher and IAI Heron from Israel, as well as the Idea Forge Switch, TAPAS-BH-201 (RUSTOM II) and DRDO RUSTOM I.

China. The PLA Navy has been actively involved in conducting experiments with intelligent and autonomous surface warships, as well as underwater vehicles. The Haiyi, also referred to as the Sea Wing, is an underwater glider that has primarily been employed for scientific

endeavours. Currently, PLAN is utilising the 'Jinghai', a warship equipped with AI-enabled navigation capabilities.

Iran. Iran's objectives in the field of AI revolve around the strategic integration of various platforms, aiming to establish a centralised command and control system that enhances the efficiency of decision-making processes. The recently developed Iranian drones possess the capability to function through AI systems.

Turkey. The defence sector in Turkey is increasingly adopting AI. Turkey has established collaborations with multiple academic institutions currently to undertake four AI projects. The military is set to acquire a total of 500 autonomous drones commonly referred to as "kamikaze" drones in which a range of AI-enabled drone, such as the Togan, Alpagu and Kargu, exist.

Israel. IDF employ a strategic approach that is grounded in the conviction that data and AI play a crucial role in achieving victory in future war. The integration of AI into various systems, including guns, bombs, and other platforms, is becoming more prevalent among Israeli defence businesses. Israel has already developed AI enabled small ship and Drone (Hebron).

Role of AI in Ukraine War. The utilisation of AI by the Armed Forces of Ukraine facilitates the processing of data, analysis of the battlefield condition and selection of targets for offensive actions. Ukraine has implemented facial recognition software developed by Clearview AI, a company based in the United States. AI is assuming a significant role in the domains of EW and cryptography. On the other hand, in numerous instances, Russia has rendered Western technologies employed by Ukraine ineffective. Both Russia and Ukraine have incorporated AI-enabled drones into many aspects of warfare.

Deduction, Implication and Gain of the Case Study for BN. The utilisation of AI in contemporary combat is exemplified by the deployment of drones, UAVs and other similar technologies in the Nagorno-Karabakh Conflict and Ukraine War. All the countries included in the case study have conducted extensive research, development, and experimentation pertaining

to various uses of AI. Most of the developed navies have followed the 'Explore-Decision Making-AI Strategy-Investment-Development' cycle in adopting 4IR Technology vis-à-vis AI and Big Data Application. Same cycle may be applicable for BN in adopting AI and Big Data Application.

Integrating AI and Big Data Application in Bangladesh Navy

Present State of AI and Big Data Application in Bangladesh Armed Forces. Recently the requirement of AI and Big Data Analysis implementation in the Bangladesh Armed Forces has been considered. As such AI policy formulation is under active consideration. Bangladesh Army has taken project for introducing AI based War gaming simulator under ARTDOC. BN has introduced few AI based projects like Combat Management System, Machinery Control System and Face Recognition systems. But none of the forces has taken any project based on Big Data. Bangladesh Air Force has not taken any step yet to implement AI and Big Data in any of their projects. Joint effort by all three services is paramount in implementing AI application like Joint Service IFF Centre.

Present State of AI and Big Data Application in BN. The application of AI in BN is now limited; therefore the "Centre for Naval Research and Development" (CNRD) is conducting small-scale research. A few officers are engaged in R&D on a project based on a "Self-Targeting Autonomous Gun Control System" that interface with radar outside of the core CNRD supervision. Similarly, Present State of Big Data Application in BN is very limited despite lot of potentiality.

BN's Assessment for Integrating AI and Big Data Application. Thorough examination and assessment are vital in order to gauge the performance, dependability and efficacy of AI and Big Data applications within the operational setting of the BN. Developing a strategy will allow BN to identify specific areas where AI and big data can be applied. Such strategy will ensure that these data assets are properly collected, managed and utilized. A well-defined strategy will enable the integration of AI and

big data applications into decision support systems, enabling BN personnel to make more informed and timely decisions.

BN's Resource Requirements for Integrating AI and Big Data Application. BN's Resource Requirements for Integrating AI and Big Data Application are as follows:

- **Data Infrastructure.** Robust data infrastructure is essential for the integration of 4IR Technology in BN which includes data storage capacity and high-performance computer.
- **Data Collection and Management.** BN needs to invest in data collection systems and technologies that can capture relevant and accurate data from diverse sources.
- **Computing Resources.** BN needs to allocate resources for high-performance computing systems, including servers, processors, and GPUs (Graphics Processing Units).
- **Skilled Personnel.** BN needs to invest in training programs and recruit skilled personnel to develop AI and big data systems.
- **Partnerships and Collaboration.** BN should actively seek collaborations to leverage external resources and stay at the forefront of AI and big data integration.
- **Testing and Evaluation.** Adequate resources should be allocated for testing and evaluating AI and big data applications in BN.
- **Regulatory and Ethical Compliance.** Resources should be allocated by BN to ensure compliance with regulations, laws and ethical considerations related to AI and big data applications.
- **Budgetary Allocation.** BN needs to allocate budgets for research and development, infrastructure upgrades, technology acquisition, training programs, and ongoing maintenance and support of AI-automation and big data analytics.

Potentials and Challenges of BN in Adopting AI and Big Data Applications

Potential Fields for Adopting AI and Big Data Application in BN. BN has the potential to adopt AI and Big Data technologies. The adoption of 4IR technologies in BN comes with challenges, as mentioned earlier.

- **Surveillance at Sea.** AI and Big Data help detect and identify threats, monitor maritime activities, and provide real-time updates to naval commanders.
- **Autonomous Systems.** Autonomous platforms possess the ability to function autonomously, hence enabling them to engage in independent operations and execute a range of duties, including but not limited to surveillance, reconnaissance and various other functions.
- **Command and Control.** AI can assist naval commanders in making informed decisions by providing real-time analysis, predictions, and recommendations.
- **Cyber Security.** AI has the potential to be utilised in the field of cyber security for the purpose of identifying and addressing cyber threats.
- **Combat Management System (CMS).** AI can optimize CMS. By analysing historical maintenance data, operational parameters, and real-time information, AI algorithms can increase operational readiness and cost savings by CMS.
- **Training and Simulation.** AI algorithms can generate intelligent adversaries, simulate realistic scenarios, and provide feedback and analysis to train naval personnel, enhancing their skills, decision-making abilities, and readiness for real-world operations.
- **Personnel Performance and Readiness.** Big Data Analytics can be used to analyse data related to personnel training, performance and health.
- **Intelligence Analysis.** Big Data Analytics can enhance intelligence analysis capabilities of BN.

- **Ship's Machinery and Auto Pilot.** By analysing data on fuel consumption, operational patterns, environmental conditions and vessel performance, it is possible to identify opportunities for energy savings, optimize routes by auto pilot.

Generic Challenges in Adopting AI and Big Data in BN. Generic Challenges in Adopting AI and Big Data in BN are as follows:

- **Awareness and Policy.** A policy roadmap is needed for AI adoption. The adoption of AI easy with a good understanding and legislation.
- **Infrastructure and R&D.** Expert manpower, laboratory and equipment for R&D are essential for AI adaption.
- **Training.** Recruiting and training staff to manage AI-based projects has also been discovered to be a significant problem.
- **AI Challenges in the Cyber Domain.** AI is likely to be a key technology in cyber operations. Adequate level of AI learning for defending data networks is essential.
- **Budgetary Constraints.** Limited budget allocation may be a significant challenge to AI adaption.
- **Cultural Aspect in AI Adaptation.** Culturally, Bangladesh lacks in technological advancement. Majority people are reluctant and fearful to use new technologies. Conversely, universities frequently adapt new technologies in industrialized nations. (Mahbub, 2023).
- **Ethical and Legal Challenges.** Artificial intelligence in defensive and offensive operations have fundamental ethical implications (Kleinman, 2020).
- **Survey Result on Generic Challenges.** 69% respondents agree with the Generic Challenges.

Technical Challenges in Adopting AI and Big Data in BN. Technical Challenges in Adopting AI and Big Data in BN are as follows:

- **Data Quality.** BN uses huge amounts of data from different sources, and ensuring accuracy and consistency of this data is critical.
- **Data Integration.** Integrating data from different sources can be challenging and require significant resources.
- **Security and Privacy.** AI and Big Data applications in BN involve sensitive and classified data, which require privacy and strict protection.
- **Skilled Personnel.** The acquisition and retention of proficient employees in the fields of AI and Big Data pose a considerable problem due to substantial demand within the private sector.
- **Technical Infrastructure.** The successful implementation of AI and Big Data necessitates the establishment of a robust technological infrastructure by BN, as these technologies demand substantial investments in computing hardware, software and networking equipment.
- **Change Management.** Adopting AI and Big Data technologies in the Navy may require significant changes to existing processes and workflows.

Operational Challenges in Adopting AI and Big Data in BN. Operational Challenges in Adopting AI and Big Data in BN are as follows:

- **Data Hacking and Poisoning.** AI poses serious security issues since it can be used to obtain unauthorized access to sensitive data and information. (Latif, 2023).
- **Cyber Attacks.** The increased reliance on Big Data and AI introduces cyber-attack that can be exploited by cybercriminals and adversaries.
- **Autonomous Weapons.** The establishment of explicit rules and international legislation is crucial in order to guarantee the ethical use of AI-powered weapons.
- **Misinformation and Disinformation.** The widespread availability of Big Data and AI can be exploited to spread misinformation and disinformation campaigns.

- **Over Dependency on Machinery.** Over-reliance on AI systems and machinery can create vulnerabilities, especially if there are single points of failure.
- **AI-Enabled Espionage and Sabotage.** The usage of AI in naval operations can be exploited by adversaries for espionage and sabotage purposes.

Ways Forward, Implementation of Strategies and Roadmap for BN

Ways Forward. After Data Analysis following aspects are found to be the ways forward for BN to adopt 4IR Technology, in particular, AI and Big Data:

- **Devise Suitable Strategy.** Every new venture always faces some challenges but a suitable strategy can overcome those.
- **Awareness Generation.** A high-level education through seminar and conference is required to appraise the BN leadership about AI so that they can comprehend the benefits and make decisions to incorporate AI tools for BN (Rahman P. D., 2021).
- **Policy Framework.** An appropriate policy framework should be there for the Al application in BN (FGD). BN may develop a Policy Framework so as to complement national strategy .
- **Develop a Data Strategy.** BN must identify the types of data it needs to collect and analyse, such as sensor data, satellite imagery, historical records and intelligence reports.
- **Invest in Technical Infrastructure.** BN needs to invest in high-performance computing systems, storage solutions, networking infrastructure and data processing frameworks designed to handle the unique demands of naval operations.

- **Recruit and Retain Skilled Personnel.** BN needs to recruit and retain professionals with expertise in data science, machine learning, AI algorithms, big data analytics and cyber security.
- **Budget.** Allocating sufficient budgetary resources is critical for BN to support its AI and big data initiatives. Funding should be allocated to procure necessary hardware, software, and infrastructure required for data storage, processing and analysis (Latif, 2023).
- **Embrace Cloud Computing.** Cloud computing will offer significant advantages to BN in terms of scalability, flexibility and cost-effectiveness. BN can leverage cloud service providers' infrastructure, enabling them to store, process and analyse large volumes of data efficiently.
- **Prioritize Privacy and Security.** In BN, prioritizing privacy and security are of paramount importance when working with AI and big data as naval data often includes sensitive information.
- **Establish Partnerships.** Establishing partnerships with relevant organizations and institutions can enhance BN's capabilities in AI and big data.
- **Foster a Culture of Innovation.** Creating a culture of innovation is vital for BN to fully exploit the potential of 4IR Technology.
- **R&D.** In order to identify the use of AI-based technologies and processes that can satisfy demand, BN must support R&D. R&D, prototyping, lab testing, field testing, and deployment are the several stages that must be completed before BN may adopt AI (Rahman D. A., 2023).

Proposed Strategy for Adopting AI and Big Data in BN. Proposed Strategy for Adopting AI and Big in BN is shown in table 1.

Table 1: Strategy for Adopting AI and Big Data in BN	
Focus Area	**Strategy**
Define Objectives	• Clearly define the objectives and goals for adopting AI and Big Data in BN. • Prioritize objectives based on potential impact on operations.
Assessment and Needs Analysis	• Conduct a comprehensive assessment of BN's current capabilities, data assets and technology. • Identify specific areas where AI and Big Data can bring value.
Data Collection and Management	• Invest in robust data collection and storage infrastructure. • Develop data governance policies and procedures.
AI and Machine Learning Integration	• Build AI and ML capabilities tailored to naval operations. • Implement AI models for predictive maintenance, anomaly detection, operational optimization and training.
Analysis	• Implement Big Data analytics platforms to process and analyze large volumes of data in real-time. • Use analytics to gain insights into threat detection and mission planning.
Cyber security Measures	• Strengthen cyber security protocols to protect sensitive AI and Big Data systems. • Conduct regular security audits and invest in advanced security technologies.
Collaboration and Partnerships	• Collaborate with other military branches, defense contractors and research institutions to share knowledge and resources. • Consider partnerships with tech companies specializing in AI and Big Data solutions.

Table 1: Strategy for Adopting AI and Big Data in BN	
Focus Area	**Strategy**
Human Capital Development	• Invest in training programs to up skill naval personnel • Create career paths and incentives for officers and technicians specializing in AI and Big Data.
Testing and Evaluation	• Conduct rigorous testing and evaluation of AI and Big Data. • Continuously refine and improve these systems based on performance metrics.
Ethical and Legal Considerations	• Develop policies and guidelines for the ethical and legal use of AI and Big Data in naval operations.
Budgeting and Funding	• Allocate funding for AI and Big Data initiatives. • Seek additional funding through government grants.
Culture Shift	• Promote a culture of innovation and AI decision-making. • Encourage openness to new technologies.
Monitoring and Reporting	• Establish Key Performance Indicators (KPIs) to monitor
Future-Proofing	• Design AI and Big Data systems to be adaptable to future technological advancements.
Evaluation	• Continuously evaluate the effectiveness of AI and Big Data applications and adjust as needed. • Stay updated on the latest developments in AI and Big Data to remain at the forefront of innovation.
Source: Author Construct	

Proposed Roadmap for Adopting AI and Big Data in BN. Proposed Roadmap for Implementing AI and Big Data Strategy.

Table 2: Roadmap for Adopting AI and Big Data in BN

Term		Strategic Focus Areas	Actions
Short Term	[Upto 5 Years]	Explore, Assess Need and Define Objectives	• Explore potentiality of BN • Conduct a thorough assessment of the BN's current capabilities, infrastructure and data availability • Identify specific areas where AI and Big Data can bring value • Define clear and measurable objectives for each area of application
		Conduct Benchmarking	• Conduct benchmarking to gain an understanding of 4IR technologies and its applications in BN.
		Decide to Develop a Data Strategy	• Decide to develop strategy • Create a comprehensive data strategy that outlines how the navy plans to collect, store, manage, analyze, and leverage data. • Define data governance policies specific to naval operations. • Identify data sources and ensure compliance of privacy and security regulations.
		Establish a Cross-Functional Team	• Assemble a multidisciplinary team of experts, officers, specialists and data scientists who will develop strategies and implement Big Data and AI-related issue.

Table 2: Roadmap for Adopting AI and Big Data in BN			
Term		**Strategic Focus Areas**	**Actions**
		Allocate Budget	• Setting up Big Data and AI-related naval warfare infrastructure involves various budgetary aspects. • Research and Development (R&D). Developing such technologies for BN requires significant investment in R&D. • Hardware and Software. To support the applications, BN need to invest in specialized hardware and software infrastructure. • Data Acquisition and Processing. The systems need to acquire relevant and diverse datasets, data processing and storage infrastructure. • Testing and Evaluation. Adequate funding should be allocated for testing and evaluating the systems. • Cyber security. Budgeting for advanced cyber security systems, encryption, intrusion detection should be considered. • Training and Education. Investing in training for personnel involved in Big Data and AI-related naval operations is crucial. • Maintenance and Upgrades. Such systems require regular maintenance and upgrades to keep them up to date and optimize their performance. • Scalability and Future Expansion. Budget planning should consider scalability and future expansion requirements.
		Develop Pilot Projects	• Start with small-scale pilot projects to test and validate AI and Big Data solutions in real-world naval scenarios. • Evaluate the performance and impact of the pilot projects against defined objectives.

Table 2: Roadmap for Adopting AI and Big Data in BN			
Term		**Strategic Focus Areas**	**Actions**
Mid Term	[5 to 10 Years]	Develop Skilled Workforce and Trained	• Recruit and train personnel with expertise in AI algorithms and big data analytics • Establish recruitment programs to attract professionals including training
		Invest and Build Technical Infrastructure and Resources	• Invest in the necessary technical infrastructure to support AI and Big Data initiatives. • Consider factors like data processing speed, scalability, reliability and security.
		Establish Data Partnerships	• Forge partnerships with research institutions and industry leaders to access 4IR technologies and data resources. • Collaborate on research projects, and joint development of AI and Big Data solutions tailored to naval requirements. • Engage with technology vendors to leverage expertise for innovative solutions.
		Prioritize Security and Privacy	• Ensure protection from cyber threats. Implement authentication mechanisms. • Adhere to protection regulations and ethical guidelines • Embed privacy considerations into AI and Big Data initiatives.
		Scale-Up and Deploy	• Once successful pilot projects are identified, scale up the deployment of AI and Big Data solutions across BN. • Develop a roadmap for phased implementation of AI and Big Data

Table 2: Roadmap for Adopting AI and Big Data in BN

Term		Strategic Focus Areas	Actions
Long Term	[10 to 15 Years]	Foster a Culture of Innovation	• Encourage a culture of innovation within the navy by promoting collaboration, knowledge sharing and experimentation. • Provide platforms for personnel to propose and develop innovative AI and Big Data projects. • Recognize and reward successful initiatives to motivate further innovation.
		Continuously Learn and Adapt	• Stay abreast of the latest 4IR technologies and their applications in naval operations. • Invest in continuous learning programs to keep personnel up to date. • Adapt the strategy based on new opportunities and lessons learned.
		Evaluation and Continuous Improvement	• Establish mechanisms for evaluating the performance, effectiveness, and impact of such systems in real-world naval operations.

Source: Author Construct

Recommendations

The paper shows that the AI adaptation strategy will be a viable option for Bangladesh. To implement the strategy following actions are recommended:

- BN may take necessary action to materialize the short, mid and long-term plans as described in the strategy to implement the roadmap.
- BN may pursue at appropriate level including MOPT & ICT to issue guidelines in National AI Strategy for BD Armed Forces and BN.
- A committee may be formed comprising representatives from BN, civilian experts, industrialists and universities for assessing, updating and devising implementing strategy of proposed strategic roadmap.
- BN may recruit experts for effective R & D, training and setting modalities for BN.

- Efforts may be taken by BN to empower concerned directorate for conducting research on application of AI and Big data Analytics in naval warfare domain and develop indigenous capability.
- Efforts may be taken by BN to arrange training from friendly countries and make cooperation agreement to prepare BN personnel to adopt 4IR technology.
- Efforts may be taken at policy level to bring synergy among BD Armed Forces, civilian industrialists and techno-universities in the field of budget sharing, R&D, training, development, standardization of equipment and increasing interoperability.

Conclusion

AI can be leveraged to optimise the performance of sensors and weapons. The security system, combat management system, fire control system, search radar, automated navigation system, sonar system, missile system, torpedo system, and machinery control and monitoring system are just a few of the systems that BN is exploring integrating AI into. Additionally, BN is exploring use of huge data collected from different sources, with the aim of improving decision-making processes. It is imperative for BN to prioritise education in this particular field in order to adequately equip BN personnel with the necessary skills to effectively embrace and utilise such technology. Coordinated efforts among BD Armed Forces in the field of R&D, resource development, standardization, training, etc. will enable effective adoption in BN.

The research indicates that the adoption of 4IR technologies, specifically AI and Big Data will yield favourable outcomes in areas such as decision making, data analysis, ISR and addressing AI-based threats. In order to achieve the desired outcome, it is imperative for BN to establish a comprehensive awareness campaign, formulate a strategic roadmap, allocate sufficient budget, foster collaboration with industry experts and cultivate a skilled workforce. The research has proposed a comprehensive strategy and roadmap for effectively integrating artificial intelligence and big data in the field of battle networks.

References

1. Allen, G. & Chan, T.,2017. Artificial Intelligence and National Security. Cambridge: Belfer Center, Harvard Kennedy School.
2. Andriole, Stephen J. & Hopple, Gerald W.,1988. Defense Applications of Artificial Intelligence: Progress and Prospects [Online] Available at: https://searchworks.stanford.edu/view/1308584 [Accessed 26 February 2023].
3. Borek, Alexander & Prill, Nadine, 2020. Driving Digital Transformation through Data and AI: A Practical Guide to Delivering Data Science and Machine Learning Products, Kogan Page.
4. Bowers, Dr. Ian & Kirchberger, Dr. Sarah, 2020. Not So Disruptive After All: The 4IR, Navies and the Search for Sea Control. [Online] Available at: https://www.tandfonline. com/doi/full/10.1080/01402390.2020.1848819 [Accessed 23 February 2023].
5. Das, Amit, 2022. Submarine Warfare & Artificial Intelligence [Online] Available at: https://www.financialexpress.com [Accessed 24 February 2023].
6. Davenport, T. H. (2018). The AI Advantage. London: MIT Press.
7. Del Monte, Louis A. 2018, Genius Weapon: Artificial Intelligence, Autonomous Weaponry and the Future of Warfare [Online] Available at: https://www.goodreads.com/en/book/show/40604739 [Accessed 26 February 2023].
8. Dhiman, Mehak, 2020. The Role of Artificial Intelligence in The Navy [Online] Available at: https://maritimeindia.org [Accessed 26 February 2023].
9. Dutta, Cdr Subhash, 2020. Artificial Intelligence and Machine Learning for The Indian Navy [Online] Available at: https://maritimeindia.org [Accessed 25 February 2023].
10. Galdorisi, George & Tangredi, Sam J., 2021. The Importance and Applications of Artificial Intelligence to Naval Operations

[Online] Available at: https://mscconference.com/wp-content/uploads/2021/04 [Accessed 25 February 2023].

11. Islam, C. Nazrul, 2021. Artificial Intelligence in Warfare: Adaptation Strategies for Bangladesh Navy, Dhaka: AFWC, NDC.
12. Kulshrestha, R A. Dr. S., 2017. Big Data Analytics in Indian Navy [Online] Available at: https://www.academia.edu/78921028 [Accessed 27 February 2023].
13. Kulbiej, Eric & Wolejsza, Piotr, 2017. Naval Artificial Intelligence [Online] Available at: https://www.researchgate.net/publication/318655874 [Accessed 24 February 2023].
14. Layton., Dr. Peter, 2021. Winning the Ai-Enabled War-At-Sea [Online] Available at: https://www.maritime-executive.com/editorials [Accessed 25 February 2023].
15. Mclemore, Connor S. & Lauzen, Hans, 2018.The Dawn of Artificial Intelligence In Naval Warfare [Online] Available at: https://warontherocks.com/2018/06 [Accessed 24 February 2023].
16. Mukherjee, Tuneer, 2018. Securing the Maritime Commons: The Role of Artificial Intelligence in Naval Operations [Online] Available at: https://orfonline.org/wp-content/uploads/2018/07/ORF_Occasional_Paper_159_AI-Naval.pdf [Accessed 25 February 2023].
17. Rana, R. K. & Chhabra, S.,2019. Challenges for Developing Navies to Adopt Industry 4.0 [Online] Available at: https://www.researchgate.net/publication/338292508 [Accessed 24 February 2023].
18. Shakhuja, Vijay, 2021. Fourth Industrial Revolution Technologies: Maritime and Naval Operaions, Pentagon Press, New Delhi, India
19. Stone, P., 2016. Artificial intelligence and life in 2030. California: Stanford University.
20. Stuart J. Russell & Norvig, Peter, 2009). Artificial Intelligence: A Modern Approach (3rd edition). New Jersey: Pearson Education, Inc.

21. Tangredi, Sam J. & Galdorisi, 2021. George, AI at War: How Big Data, Artificial Intelligence, and Machine Learning Are Changing Naval Warfare, Naval Institute Press, Annapolis, Maryland

22. Tuang, Nah Liang, 2021. The Fourth Industrial Revolution's Impact on Smaller Militaries [Online] Available at: https://www.jstor.org/stable/resrep19925.pdf [Accessed 23 February 2023].

23. Vincent O'Hara, L. H., 2022. Innovating Victory: Naval Technology in Three Wars. s.l.:US Naval Institute Press. [Online] Available at: https://oceanofpdf.com/authors/vincent-p-ohara/pdf-epub [Accessed 23 February 2023].

24. Zysk, K., 2020. Defence innovation and the 4th industrial revolution in Russia. Defence innovation and the 4th industrial revolution in Russia.

Author

Commander Mahbuba Afroze, (L), afwc, psc, BN was commissioned on 21 December 2001 in Electrical Branch. She completed her Network Manager Course from India and Specialization from BNS SHAHEED MOAZZAM. She also did course on C802A SSM from 3rd Academy, Beijing, China. She has served onboard various ships, bases and Dockyard of Bangladesh Navy in different capacities. Some of her appointments include GPE (L), Design Engineer and DGM(P&E) at BN Dockyard, DDNIT at NHQ, System Analyst and Senior Maintainer at SMWT, and Electrical Officer of BNS UMAR FAROOQ, BNS OSMAN and BNS ALI HAIDER. The officer attended Junior Staff Course in BNA and Principle Staff Course from DSCSC, Mirpur. She is married to Commodore M Zillur Rahim Khan and blessed with a daughter.

NDC JOURNAL
Security Through Knowledge

UNMANNED AERIAL VEHICLE IN WARFARE: CHALLENGES IN AIRSPACE MANAGEMENT IN BANGLADESH

Group Captain Salah Uddin Md Alim-Al-Rabbi
GUP, afwc, psc, GD(P)

"The proliferation of drones presents significant challenges to global security and requires careful management and regulation."

- Ban Ki-moon, Former Secretary-General of the United Nations.

Introduction

Unmanned Aerial Vehicle (UAV) is a pilotless aircraft, which is flown without a pilot-in-command on-board and is either remotely and fully controlled from another place (ground, another aircraft, space) or programmed and fully autonomous (AFD, 2019). UAVs have become an integral part of modern warfare, as they offer unique advantages in intelligence, surveillance, target acquisition and reconnaissance (ISTAR). Their success was aided by their ability to avoid detection and destruction by conventional air defense (AD) systems (Dr Ahmed, 2022). However, the use of UAVs in warfare also presents challenges in airspace management (ASM), particularly in countries like Bangladesh (BD), which have limited resources and infrastructure for monitoring and controlling airspace. Whereas ASM prevents all airspace users from interfering with one another, facilitates identification and AD and ensures the safe flow of all air traffic.

Civil Aviation Authority of Bangladesh (CAAB) is primarily responsible to promulgate necessary regulations and guidelines for ASM. Accordingly, CAAB has promulgated an official circular on this issue titled 'Civil Aviation Circular on Operating Remotely Piloted Aircraft Systems' in January 2019' and other regulations in line with the guidelines of International Civil Aviation Organization (ICAO). The circular has broadly touched upon

major points keeping UAV operations restricted in mainly segregated airspace which may limit the use of potential UAV operations. Again, in the event of an emergency or war, Bangladesh Air Force (BAF) will assume responsibility for ASM. At this backdrop, proliferation of UAV use will pose challenges and threat to ASM in BD. Despite the huge potentials of UAV, appropriate ASM procedures are necessary to ensure effective employment of UAV.

Review of Literature

The literatures which are reviewed before embarking to this research are mostly confined to the types, capabilities, concept of operations, employment of UAV in warfare, circulation of civil aviation authority, ASM theory and concepts etc as no research has been carried out about challenges of ASM considering UAV operations.

CAAB in the circular titled 'Circular on Operating Remotely Piloted Aircraft Systems (RPAS)' governs the Unmanned Aircraft System (UAS) operations in BD.

ICAO in the circular titled 'Cir 328 AN/190 on UAS' describes UAS as cutting-edge technology which needs to be integrated with all civil aviation flying. This circulation does not talk about ASM in war like or crisis scenario.

'Draft Doctrine for UAS Operation' discusses the different categories of UAVs, role, task and employment of UAS. It briefly covers few ASM issues for peace time only.

A.R.Jha in his book titled 'Theory, Design and Applications of Unmanned Aerial Vehicles' mostly covers the theoretical aspects of UAV and does not explain the ASM aspects.

Study report on 'Drones in the Ukrainian War will They be an Effective Weapon in Future Wars' by Dr. Ahmed Daifullah al-Garni, article 'The Impact of the Nagorno-Karabakh Conflict in 2020 on the Perception of Combat Drones' etc were reviewed to find out the ASM challenges during different wars.

From the review of literature, it is evident that literature focusing on challenges of ASM concerning UAV is meagre in number. However, some of the reviewed literatures have contributed to understand ASM challenges in a congested airspace like BD. The joint coordination among UAV operators of different services is also not explored. To bridge the identified knowledge gap, a deliberate study is required to determine the challenges of ASM with the proliferation of UAV in warfare and its mitigation measures.

Methodology

For writing this article, an exploratory type of research was conducted. The scope of this research was limited to military UAV only. The study is based on the theoretical approach and limited operational experience of Bangladeshi UAV operators. A total of 17 interviews were conducted with concerned officers from three services, Armed Forces Division (AFD) and CAAB. A Focus Group Discussion (FGD) consisting of 07 concerned officers from BAF was also conducted. Secondary data was collected from pertinent documents, articles, research reports etc. The data collected through the field survey, document study and interview method were subjectively analyzed to derive necessary logical explanations of concepts and see the linking phenomenon or arguments to attain the objectives of the research.

Capabilities and Operational Requirement of UAV

Projected Capabilities of UAV from Resent Wars. Armed UAVs have been used by the United States (US) and its western allies in the hybrid and uncontested battlefields in Afghanistan, Palestine and Iraq for nearly two decades. Non-western major actors such as Russia, China, Turkey, and Iran have recently produced and those Armed UAVs are employed in various conventional battlefields such as Syria, Libya, Armenia, and, most recently in Ukraine. Following capabilities were found from the above-mentioned wars:

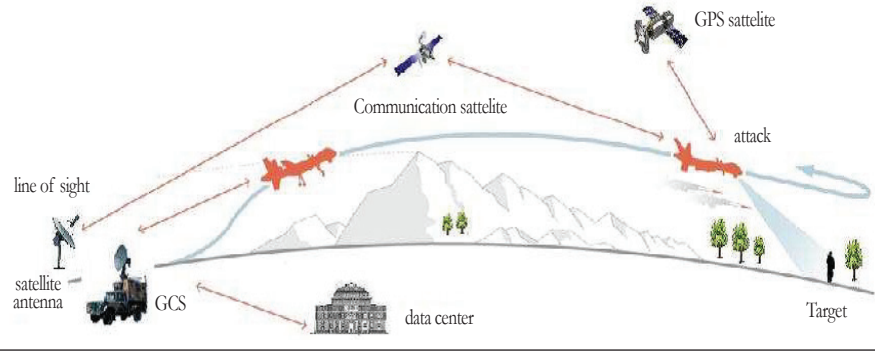
- Intelligence, Surveillance and Recconnaisance (ISR).
- Ground Attack.

- Search and Rescue.
- Ground Mapping.
- Border Patrol.
- Communication Relay Station.
- Target Acquisition and Designation.
- Target Illumination.
- Correction of Artillery and Naval Gun Fire Support.
- Transportation of Small Critical Items.
- Survey of Maritime Area.
- Electronic Warfare (EW).

Requirements of UAV Operations. UAV operates integrating a system of systems. If any of the subsystems fails, the UAV will not operate effectively. Subsystems of UAV are as follows:

Ground Control Station (GCS). It is the controlling station from where UAV is controlled from ground. It may be as large as a container box, or a mobile command centre or a small device like tablet or mobile set. GCS needs to be placed from where line of sight (LOS) remains clear with UAV. GCS receives all data and video from the UAV and the same can be relayed to command or operations centres (Figure 1).

Figure 1: Communication System of UAV



Source: Gheorghe UDEANU, 2016

Pilots and Operators. These are the human operators in charge of piloting the UAV and operating different sensors from the GCS. Mainly

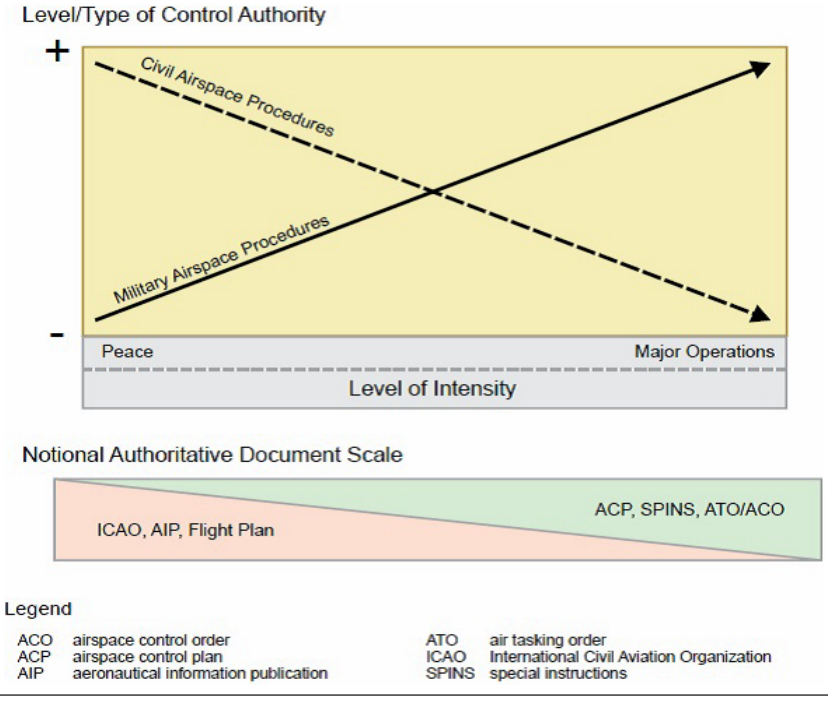
'Medium-Altitude Long Endurance (MALE)' and 'High-Altitude Long Endurance (HALE)' class UAV may require both pilots and operators.

Take-off/ Launching and Landing System. If the UAV is not launched and landed using conventional take-off and landing from a runway, a launch and landing mechanism would be required.

Existing ASM Regulations for UAV Operations in BD

Notional Airspace Control Authority. ASM of BD is carried out by both CAAB and BAF. Most of the countries follow the similar approach for ASM. The "Notional Airspace Control Authority" Figure 2 illustrates the various intensities of civil and military operations and their corresponding control authorities (US Air Force, 2021).

Figure 2: Notional Airspace Control Authority



Source: Air Force Doctrine Publication 3-52, Airspace Control, US Air Force

CAAB Circulation 2019. UAV flying in BD airspace requires permission from the CAAB and other relevant authorities. CAAB issued the circular to make UAVs as legitimate airspace users. Some of the important aspects of this circulation are as follows:

- The pilot operating shall maintain continuous unaided visual contact with the UAV sufficient to be able to maintain operational control.
- The pilot shall operate not more than one UAV at any one time.
- The pilot operating a UAV shall give way to all manned aircraft.
- The maximum height for operations of UAV shall be 200 ft Above Ground Level (AGL).
- The operation of UAV is prohibited within 10 nautical miles (NM) of an aerodrome and within 05 NM of a Key Point Installation (KPI), built up area, sensitive government installations.
- Full automation of UAVs is not permitted.

Drone Registration & Flying Regulation, 2020. This policy entails different regulations related to registration of UAV by civil users as well as highlights some flying regulations. It describes three drone operations zone as follows:

- **Green Zone (no permission is required).** UAV can be operated at 50 ft height maximum at 3 to 5 km distance from airport/KPI and maximum at 100 ft height beyond 5 km distance from airport/KPI.
- **Yellow Zone (require permission to operate).** Restricted areas, military areas, populated areas, and congested areas are included in this zone.
- **Red Zone (require special permission to operate).** Prohibited areas, dander areas, airport/KPI and special KPI are included in this zone.

Air Navigation Order (ANO) on UAV Operations. ANO on (UAV) CAAB Part 947 and Part 945 is the latest order published on 15 November 2021. The volume of 160 pages covers the regulations of flying, pilot

licencing, maintenance, risk management, emergency handling etc. This ANO divides 'Categories of UAS Operations' into three categories, those are, 'Open', 'Specific' and 'Certified'. Summary of operations based on risk of the above-mentioned categories are shown in Table 1.

Table 1: Operation of Category Based on Risk

		
Open Category- Low Risk, No Pre-approval, Limitations: 5 KG, Visual Line of Sight (VLOS), 100 ft height. System of zones 2 Subcategories: Fly close/over people and Far from People	Specific Category - Increased Risk. Certifications of UAV – As Specified. Certification of Pilots - Specific UAV Operator Certificate (ROC)	Certified Category - Risk as manned aviation. Certifications of UAV – As Certified. Certification of Pilots - Certified UAV Operator Certificate (CROC)
Recreational purpose, model flying, non-commercial photography	Beyond Visual Line of Sight (BVLOS) operations, aerial work, cinematography…etc	Air taxi, package delivery
Source: CAAB ANO, 2021, p. 9		

Comparison of UAV Operation Regulations. Important aspects of UAV Operation Regulations of BD, India and Singapore are given in Table 2. In BD, the maximum allowable operating height for UAV is 200 ft which is further reduced to 100 ft in ANO. India allows a maximum of 400 ft. Most of the helicopters and other manned aircraft in BD operate at or

above 500 ft for low level flying or enroute. Such restrictions limit the integration flexibility of UAV with manned aircraft into national airspace.

Table 2: Comparison of UAV Operation Regulations

Criteria	BD	India	Singapore
Maximum allowable operating height	100 ft (ANO)	400 ft	200 ft
Minimum clearance from building, structure, vehicle and person	1000 ft	2km	Not specified
Minimum clearance distance from KPIs	5/3km (ANO)	5/3km	5km
Minimum clearance from aerodrome	5/3km (ANO)	5/3km	5km
Pilots Training	Specified (ANO)	Specified	Not mentioned
Submission of application for obtaining approval for operation	7 working days (ANO)	7 working days	Not specified
Automated system for obtaining permission	No	Yes	No
Clearance from international border	Not mentioned	25km	Not mentioned
Unmanned Traffic Management	No	Yes	Yes

Source: (CAAB Circular, 2019) (CAAB ANO, 2021) (DGCA India, 2021) (CAAS, 2023)

Existing War Time ASM Regulations for UAV Operations

Positive Control. It is based on real-time data obtained through the use of facilities such as primary radar, secondary radar, and associated communications. Positive control becomes difficult for UAV due to its low Radar Cross Section (RCS).

Procedural Control. It relies on a combination of orders, procedures, rules, and measures that have been previously agreed upon and promulgated. As radar is unable pick-up UAV most of the time, procedural control remains as a backbone for UAV control.

Airspace Control Order (ACO). It specifies the airspace control measures (ACM), including information on AD resources, sensors, and shooters, as well as their activation times, altitudes, specific locations, and routes and corridors used by friendly aircraft across the theatre of operation.

Limitations of UAV Operations

Height and Lateral Distance Limit of Segmented Airspace. Maximum 100 ft height limit and 1000 ft lateral distance may not meet the requirement of UAV operators most of the time.

Unmanned Traffic Management (UTM) Framework. UTM framework is not yet planned. Thus, UAV need to be instigated well with the manned aircraft in the existing manual Air Traffic Management system (ATM).

Regulations for Military UAV Operations. A common set of regulations for military users is necessary for safe integration and efficient operations.

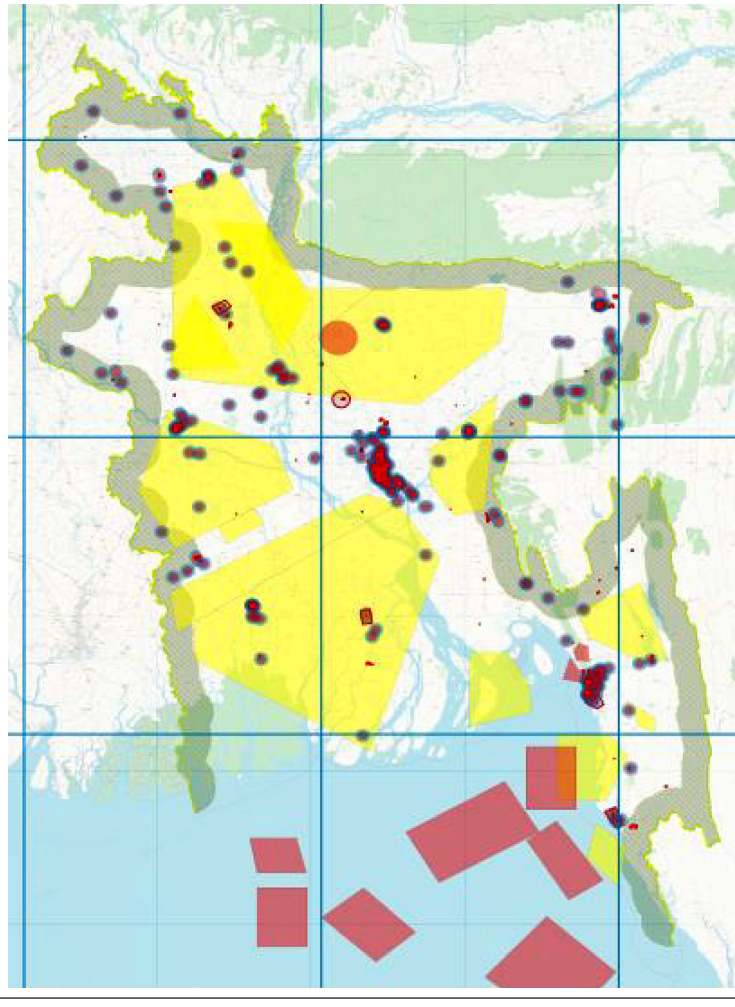
Positive Detection Capability. Most of the UAV cannot be picked-up by radars.

Challenges in ASM in Bangladesh

Detection Capability of AD and Air Traffic Services (ATS) Radar. Most of the UAVs are made with stealthy characteristics and their RCS generally < 1. Thus, the AD and ATS radar hardly can pick-up MALE/ HALE category UAVs at low level and able to detect same categories UAV flying at medium or high level

Limited Airspace of BD. Most of the airspace over the land area are declared restricted/danger/prohibited areas. In remaining corridors domestic and international air routes are planned. Thus, the limited airspace does not offer flexibility to the planners and the operators. UAS Airspace Map is given as Figure 3 where boxes and circles in different colours depicts the restricted/danger/ prohibited areas and KPIs of BD.

Figure 3: UAV Airspace Map



Source: CAAB ANO, 2021

UAV Operation from Busy Airfield. Hazrat Shahjalal International Airport (HSIA), Dhaka and Shah Amanat International Airport (SAIA), Chattogram are the busiest two airfields in the country due to civil, military and international traffic. Besides, Jashore airfield also a busy airfield due to domestic flight operation and extensive military flying by BAF Academy. Table 3 shows the comparative data of civil and international flight operations in different airfields.

Table 3: Summary of Flight Operations from Different Airfields

Ser	Name of Airfield	Total Take-off & Landing (Daily Average)			Runway Length & Width (in ft)
		Domestic	International	Others	
1	Hazrat Shahjalal International Airport (HSIA)	170	142	38	10,500x150
2	Shah Amanat International Airport (SAIA)	26	24	06	9,000x150
3	Jashore	08	-	-	8,000x150
4	Cox's Bazar	46	-	-	9,000x150
5	Sylhet	24	08	-	10,000x150
6	Saidpur	32	-	-	60,00x100
7	Barishal	04	-	-	6,000x100
8	Rajshahi	08	-	-	6,000x100

Source: Dhaka, Chattogram and Jashore Air Traffic Control (ATC) Towers

In addition, military fighter, transport and trainer aircraft and helicopters operations also need to be facilitated from those airfields. Thus, UAV operations may have to be adjusted as per the traffic situation which may hamper the UAV mission objective.

Separation between the UAV and Manned Aircraft. There is no specific separation recommended between UAV and manned aircraft in ICAO regulations. These creates a grey area and controller tends to provide more separation with manned aircraft to ensure safety (Masud, 2023).

Manoeuvrability of UAV Versus Manned Aircraft. Manoeuvrability of UAV is restrictive than manned aircraft. In addition to the slow rate of climb or descend of UAV than that of manned aircraft some delays are also observed in control input of UAV which in turn restricts the decision-making process of the Air Traffic Control (ATC) controllers.

Mindset of Planners, Operators and Controllers. Human minds are generally reluctant to accept change and it is applicable for UAV operations as this is relatively new issue for ASM. In such scenario, planners, operations and controllers remain rigid for decision making.

Coordination among the Airspace Users. UAV operations mostly depend on procedural control which demands more coordination. Again, UAV pilots remains quite away from the actual aircraft and depends mostly on electronic devises for decision making which ultimately reduces his situational awareness. Again, coordination is necessary amongst the UAV stake holders operating from same airfield/place for effective flight planning, area and flying slot management.

Technical Failure of UAV during Busy Flying Period. The major technological challenges of UAV include the possibility of lost communication between the UAV and the on-ground pilot, failure of the command and control link, sluggish response of the UAV etc. If technical issues are observed during busy flying period that becomes very crucial for ensuring safety of manned aircraft posed by UAV.

Regulatory Framework. Developing a comprehensive regulatory framework for UAV operations is crucial. Clear rules and guidelines must be established to ensure safe and lawful UAV operations, including airspace restrictions, flight altitudes, operational procedures and certification

requirements. Establishing these regulations and ensuring compliance can be a challenge (Air Cdre Mamun, 2023).

Collision Avoidance. Integrating UAVs with other airspace users requires robust collision avoidance systems. Modern technologies such as automatic dependent surveillance-broadcast (ADS-B) and sense-and-avoid systems can help prevent potential collisions and maintain separation between aircraft.

Interoperability and Standardization. Ensuring interoperability and standardization among different types of UAVs and their associated systems can be a challenge. Harmonizing technologies, communication protocols and data exchange formats enable seamless integration and coordination among UAVs and other airspace users (Air Cdre Mamun, 2023).

Duality in ASM. In BD responsibility of ASM both on CAAB and BAF. Dhaka Area Control makes all decisions regarding civil aircraft, military transport aircraft, and helicopters outside of the restricted area, whereas Air Defence Operation Centre (ADOC), BAF control military aircraft, helicopters, and UAV inside BAF training areas and responsible for AD of whole BD airspace. This type of dual responsibility poses challenges on ASM and AD of BD airspace.

Threats to ASM in Bangladesh

Illegal Surveillance and Reconnaissance. One of the primary concerns is the unauthorized intrusion of drones into restricted airspace or sensitive areas such as airports, military installations, and government buildings for illegal surveillance and reconnaissance. It can also disrupt regular flight operations, compromise national security, or pose safety risks to the public.

Smuggling. Criminals may use UAV for dropping small payloads across the border or inside their own territory. This would pose a threat to own ASM.

Electronic Snooping. UAVs equipped with the necessary technology can manipulate or falsify electronic signals, causing disruption or confusion in the airspace.

Potential Attack Platform by Terrorist. Terrorist group successfully carried out few attacks against Israel by suing small UAVs. If terrorist group is in possession of UAV may pose threat to the ASM by attacking sensitive KPI or installation.

Mid Air Collision. If a UAV successfully spoofs its position or identity, it can potentially create collision risks by misleading other aircraft or air traffic control systems.

Indiscriminate Operation by Private UAV and Helicopter Operators. Several corporate business groups operate helicopters at low-level crisscrossing restricted areas (BAF training areas) and descend below the allotted height within congested airspace of BD. In most cases, CAAB is not in a position to monitor these flying activities and in many cases, information of these helicopters is not sent to ADOC at appropriate time. This is further complicated by indiscriminate operation of UAV specially climbing above the designated height (50 or 100 feet) without prior permission from appropriate authority. Such unauthorized flying activities and violation of height become a serious threat to ASM as well as the AD system of BD (Gp Capt Mukeet, 2023).

Mitigation Measures

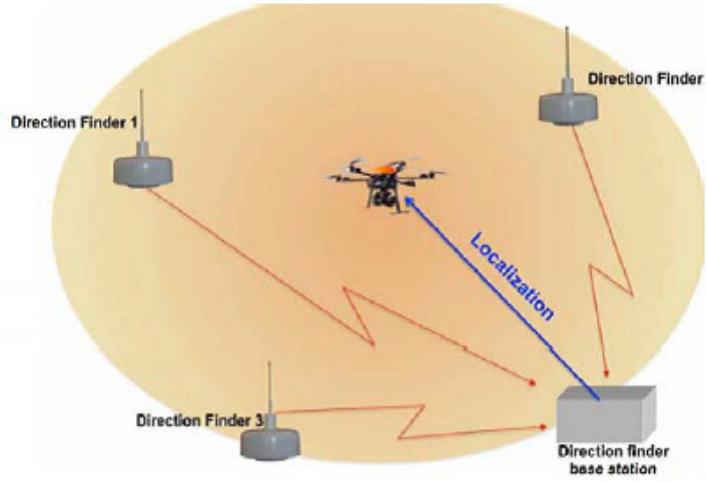
Enhancing UAV Detection Capability. UAVs possess stealthy characteristics and RCS of most of the UAVs are less than 1. Thus, it needs different technologies than manned aircraft for effective detection. Sometimes AD radar can detect MALE and HALE categories UAV at higher height. For peace time ASM, UAV may be equipped with transponder or collision avoidance mechanism like ADS-B.

Radio Frequency (RF) Emission Sensing. UAVs transmit data back to their controller via a wireless data link. This type of RF emissions can

be easily detected and located using a directional antenna or a network of synchronized ground stations. However, for the system to be cost-effective and provide rapid detection, it must have some knowledge of the emission center frequency and bandwidth (Sathyamoorthy, 2015).

Electro-Optical (EO) Sensing. EO sensors in the form of optical and thermal cameras can detect UAVs quite effectively. The Drone Tracker as shown in Figure 4 that uses optical and thermal cameras to form an EO sensing network that increases the chance of detecting a UAV.

Figure 4: Detection of UAV via EO Sensing



Source: Sathyamoorthy, 2015

Establishing Special Use Airspace. Airspace over land area almost saturated with restricted/danger/prohibited area and KPIs (Figure 3). BAF has started the process for establishing new restricted areas over the sea area focusing UAV operations. Existing restricted areas over land area may also be used by UAV operators in coordination with ADOC, and local ATC tower and Radar Station (Air Cdre Karim, 2023).

UAV Operations from Less Used Airfield. Generally MALE category UAVs can operate from 3000 feet runway. UAV operators may plan their operations from a less used runway which would provide operational

flexibility and reaction time for handling technical emergencies. Sylhet, Saidpur, Barishal, Rajshahi may be viable options for optimum utilization of UAV. Ishwardi, Lalmonirhat and Shomshernagar airfields are good options for daytime operation presently. For operating in the south and south-eastern part of the country Cox's Bazar and Barishal are likely to be good options. MALE or HALE categories UAV operation from Tejgaon airfield or Dhaka area would be highly discouraged by CAAB considering the closest proximity to Hazrat Shahjalal International Airport as well as KPIs and other sensitive areas (Masud, 2023).

Choosing UAV Operations Time when Traffic Density is Less. This is applicable when UAV would be operated from busy airfield like Chattogram or Jashore. While operating from SAIA, UAV operators need to choose the slot in coordination with Chattogram ATC Tower considering traffic density and at a time one UAV may be allowed to address the challenge of ASM.

Review of ACM with Inclusion of UAV. ACM can be divided into two - areas which friendly traffic normally avoids, and routes over which friendly ac navigate. The use of friendly weapon-systems on these routes is restricted. In the existing ACM, high-speed aircraft are planned at higher height and slow speed aircraft/ helicopters are planned at lower height. But UAVs are susceptible to ground fire at lower height and communication with GCS works better at higher height. Thus, height block for UAV in ACM needs to be specified at higher height.

Integration of Identification Friend or Foe (IFF) with UAV. In contested airspace UAV may fall pray of friendly fire. To avoid blue on blue engagement at least MALE and HALE categories UAV may be fitted with IFF (AVM Fazlul Haque, 2023). This would also facilitate better ASM during peace time.

Coordination from Single Operation Centre. Coordination can play an important role as there is no UTM system in BD. Vertical and horizontal coordination would be necessary. In existing scenario, BAF should take the

lead for conducting UAV operations in BD airspace safely (Cdre Rashed, 2023). To conduct the UAV operation safely and with better coordination from a single operation center, a 'UAV Operation Cell' may be opened at ADOC or appropriate place where representatives from BA and BN should be present.

Induction of Counter UAV System. A holistic joint approach may be followed to induct the new counter UAV system (Brig Gen Masihur, 2023) which should include the conceptual, organizational, acquisition, training, operational and the Research and Development (R&D) aspects.

Joint Doctrine for UAV Operation. Doctrine can bring alinement of concept, understanding, standardization and can also highlight interoperability of UAV amongst the services. Proposed Draft Doctrine for UAV Operations may be reviewed and published to address the plausible challenges and threats to ASM (AVM Hasan, 2023).

Geofencing. It is a location-based service in which GPS (Global Positioning System) is utilized by an application or other software. It can be either dynamically generated or predetermined around the radius of a point. Commercial UAV manufacturers can play a crucial role by incorporating GNSS (Global Navigation Satellite System)-enforced geofences into their systems to prevent their UAVs from entering exclusion zones around airports, government buildings, military installations, and other security-sensitive sites. (Sathyamoorthy, 2015).

Review of CAAB Policies and Regulations of UAV. CAAB policy/ regulations amply cover the rules and regulations for UAV operations and ASM, but all could not be tested yet by the users. Maximum height set for civil operations found lesser than neighbouring country. Again 'CAAB Circulation 2019' permits maximum height 200ft but the latest 'ANO on Drone/UAS Operations' published in November 2021 explain operations up to 100ft. Maximum height for civil users may be increased to 350ft beyond 5 km radius from airfield. However, higher capabilities UAV can also fly at higher height with special permission and rules and

regulations for those UAV will be as of any manned aircraft subject to type of operations (Gp Capt Mukeet, 2023). A 'Multi-Stakeholders Working Group' can collaborate on developing strategies, regulations and best practices for UAV integration and ASM (Air Cdre Mamun, 2023).

Introduction of UTM. It is adopted by countries like India, Singapore, Malaysia, Japan etc and most of the countries are embracing it. CAAB is far behind to embrace UTM as the project for ATM is ongoing and likely to complete by mid of 2024. Military UAV operation in BD is still limited and ATS should be able to manage the airspace through implementation of rules, regulations and vertical and horizontal coordination. However, CAAB would start the UTM implementation project upon completion of ongoing ATM project (Masud, 2023).

Recommendations

Following recommendations are made to employ military UAVs with its full capabilities by addressing the challenges and threats to ASM of BD:

- 'Multi-Stakeholders Working Group' may be formed in CAAB comprising representatives from all stakeholders, academia and relevant ministries.
- 'Joint Doctrine for UAV Operations' may be published by AFD as soon as possible.
- Military UAV operations may be planned from less used airfields like Barishal, Rajshahi, Saidpur, Sylhet (day/night) and Ishwardi, Lalmonirhat, Shomshernagar (daytime only).
- A holistic approach may be taken by AFD through services HQ to induct 'Counter UAV System' for the BDAF as soon as possible.
- Air HQ may take necessary steps to enhance UAV detection and cyber capabilities as soon as possible.
- Process of UTM framework may be started to integrate with ATM framework by CAAB as soon as practicable.

Conclusion

Employment of UAV in warfare has revolutionized modern military operations and presented both opportunities and challenges in ASM. Over the past two decades, UAV technology has rapidly evolved, providing armed forces worldwide with enhanced situational awareness, intelligence gathering and precision strike capabilities which help commanders in decision making process. In latest ANO of CAAB, height restriction of segmented airspace is 100 ft which is found unrealistic. Thus, the integration of UAVs into national airspace systems comes with a set of challenges and also pose some threats. BD as a developing country, with its existing manual ATM system is facing specific challenges in ASM with the induction of MALE category military UAVs in BD airspace recently. Therefore, identification of the challenges and threats to ASM of BD due UAV operations is necessary for taking appropriate mitigation measures to ensure employment of BDAF's UAV with its full potential.

To overcome these challenges and threats, BD needed to adopt a multi-faceted approach. First and foremost, CAAB needs to establish a multi-stakeholders working group regulatory framework taking representative from all stakeholders to balance safety, security, and operational requirements by reviewing existing rules and regulations concerning UAVs. This framework should align with international standards and best practices while accommodating the specific needs and limitations of the country. Increasing UAV detection capabilities, UAV operations from less used airfield, inclusion of aspects of UAV operations in ACM, appropriate coordination flow chain centering ADOC, induction of counter UAV system, reviewing and publishing of joint doctrine for UAV operation, introduction of UTM etc would mitigate the challenges and threats to ASM of BD. Regular evaluation and improvement of ASM practices are necessary to keep pace with technological advancements and evolving regulatory requirements. Finally, public engagement and awareness campaigns are essential to address concerns and misconceptions surrounding UAV operations. By considering these factors and implementing a comprehensive and adaptive

approach to UAV operations and ASM, UAVs can be employment with its full capabilities in airspace of BD.

References

1. AFD. (2019). Draft Doctrine for UAV Operation. Dhaka: Armed Forces Division.
2. Air Cdre Karim. (2023, June 27). Director, Air Operations, Air HQ, Dhaka.
3. Air Cdre Mamun, R. (2023, June 11). Director Air Defence. Air HQ, Dhaka.
4. AVM Fazlul Haque, A. (2023, March 12). Presentation on 'Air Power and Air Strategy: BD Perspective'. National Defence College, Mirpur, Dhaka.
5. AVM Hasan, M. (2023, June 11). Assistant Chief of Air Staff (Plans), Air HQ, Dhaka.
6. Brig Gen Masihur, M. R. (2023, April 25). Director General, Operations and Plans, AFD, Dhaka.
7. CAAB ANO. (2021). ANO on CAAB Part 947 and PArt 945 (Drone/ UAS). CAAB, Dhaka.
8. CAAB Circular. (2019). CAAB Circular on 'Operating Remotely Piloted Aircraft Systems (RPAS). Dhaka: Civil Aviation Authority of Bangladesh.
9. CAAS. (2023). Civil Aviation Authority of Singapore. Retrieved July 05, 2023, from https://www.caas.gov.sg/public-passengers
10. DGCA India. (2021). Drone Regulations 2021. Retrieved July 05, 2023, from https://www.dgca.gov.in/digigov-portal
11. Dr Ahmed, D. G. (2022). Study: Drones in The Ukrainian War will They be an Effective Weapon in Future Wars. Retrieved 23 April 2023 from https://www.scribd.com
12. Gp Capt Hayder, G. (2023, June 26). 2IC, Air Defence Operation Centre. Interview. Dhaka.

13. Gp Capt Mukeet, u.-A. (2023, June 27). Director Flight Safety and Regulations, CAAB, Dhaka.

14. Jha, A. P. (2017). Theory, Design, and Applications of Unmanned Aerial Vehicles. CRC Press, Taylor & Francis Group.

15. Masud, R. (2023, June 27). Director, Air Traffic Management, CAAB, Dhaka.

16. MOCAT. (2020, October 05). 'Drone Registration & Flying Regulation, 2020'. Dhaka: Ministry of Civil Aviation and Tourism.

17. Noor-e-Alam, G. C. (2020). Unmanned Aerial Vehicle (UAV) Operations in Bangladesh: Responses, Challenges and Threats. Dhaka: National Defence College.

18. Sathyamoorthy, D. (2015). A Review of Security Threats of Unmanned Aerial Vehicles and. Retrieved July 07, 2023, from https://www.researchgate.net/publication/282443666

19. US Air Force. (2021). 'Air Force Doctrine Publication 3-52, Airspace Control'.

Author

Group Captain Salah Uddin Md Alim-Al-Rabbi, GUP, afwc, psc was commissioned in GD(P) branch on 24 May 1999. During his commission with 38 GD(P) Course, he was awarded with 'SWORD OF HONOUR' and 'OSMANI GOLD MEDAL' (for best academic performance). He has attended various courses both at home and abroad. He was awarded with 'Chief of Air Staff Trophy' for the best performance in JCSC at CSTI BAF. He has undergone F-7 Tactical Flying Training Course in China and UN Integrated Mission Staff Officer's Course (UNIMSOC) in Canada. He is a Qualified Flying Instructor and Fighter Category 'A' pilot of F-7 Series aircraft and has logged 2532 hours. He was awarded with

'Gourobujjol Uddoyon Podok (GUP)' for his exceptional professionalism and flying performance. He has served as Instructor Pilot in BAF Academy, 5, 25 and 35 Squadron BAF and as Flight Commander (Operations) in 5 Squadron BAF. He has commanded 35 Squadron and 301 SAM Unit BAF. He is graduate from Defence Services Command and Staff College, Mirpur and Air Force Command College, PLAAF China. He has served in UN Peacekeeping Mission in DRC twice. Before joining the Armed Forces War Course, he was serving as Commanding Officer, 105 Advance Jet Training Unit (AJTU) BAF and President, Equipment Induction Team of UAV Project of BAF. He is married and blessed with a son and a daughter.

NDC JOURNAL
Security Through Knowledge

UNIVERSITY-INDUSTRY COLLABORATION FOR DEVELOPMENT OF AVIATION INDUSTRY IN BANGLADESH: CHALLENGES AND WAY FORWARD

Group Captain Sk Ashraful Hossain, afwc, psc, GD(P)

Introduction

Aviation industry encompasses the entire airline industry, maintenance and training organization including research companies to support aviation, aircraft design and manufacturing, and civil-military aviation cooperation etc. In Bangladesh (BD), there are four major components of aviation. These are air operators (scheduled, cargo and chartered airlines), service providers (air navigation, airport and security services providers), the regulator means Civil Aviation Authority of Bangladesh (CAAB); and military aviation (Hussain, 2021). In 2018, study of International Air Transport Association (IATA) shows, "current passenger could be double in air transport in Asia-Pacific region in 2037." Such expansion of aviation industry would create 2.5% of all employment (46.7 million jobs) and 3.1 % of all Gross Domestic Product (GDP) in Asia-Pacific countries (Aminul, 2022). BD has unveiled Third terminal in Hazrat Shahjalal International Airport (HSIA) partially to enhance and broaden capabilities; construction of second runway in HSIA is likely to begin next year (Hasan, 2023). Domestic air travel is now at all-time high with 25 lac passengers annually and expected to surpass 50 lacs in coming years. Government wants to resume flight operations at five Short Take-Off and Landing (STOL) airports to facilitate the growth of domestic air travel (Shams, 2023). BD aviation industry is facing challenges in acquiring required both operational and non-operational aviation professionals. Due to vastness of BD aviation industry; approved training and maintenance organization, certified operators are considered only.

There are scarcity of aviation training institutions capable of generating adequate qualified aviation professionals to meet the demand. BSMRAAU has been established to generate aviation professionals to the industry. On the otherhand, fresh graduates from various university cannot be readily employable in the aviation industry due to non-aligned and non-accredited curriculum with CAAB programme. Moreover, these graduates have to do further course for CAAB certification or proceed abroad to acquire same degree from ICAO approved universities. The existing gaps between the aviation university and industry has occurred due to not understanding the requirements of each other; means lack or non-collaboration. University-Industry Collaboration (UIC) aims to promote the transfer of knowledge and technology. UICs can take different forms, such as collaborative research and publishing, industry funding of academic researchers, academicians providing consulting services, staff conference between universities and industry, co-operation in education, internship of university graduates, and lecture by the expert industry staff (Yanikolu, 2019). BD aviation industry have not provided any significant support to BSMRAAU for skill development, resources sharing, R&D funding aspects, except conducting few seminars. Though BSMRAAU has taken few steps for the approval of CAAB of its curriculum but it's not enough. However, there was no study conducted with a holistic view to develop a formidable programme of University (BSMRAAU) - Aviation Industry collaboration.

Methodology. This is an exploratory research employing a mixed-method approach of both qualitative and quantitative data analysis. To acquire a higher perspective on the subject, Key Informant Interviews (KII) are pre-selected. A set of both semi-structured and structured questionnaires were prepared to get the qualitative data through a survey with multi-type respondents both in civil and military aviation. Focus Group Discussions (FGD) are conducted as content analysis with the subject matter expert of BSMRAAU, CAAB and different Airliners to gain an in-depth understanding on the probable challenges and ascertain the probable ways out of UIC. Secondary data are collected from the subject-related previous research paper and related documents, various books,

newspapers, journals, periodicals, and information available in authentic online open sources are used. Data collected from both primary and secondary sources has been analyzed qualitatively and quantitatively using logical deductions. All relevant data are organized in order to construct logical arguments. This study has primarily established this connection and suggested the ways out to overcome the challenges of developing required aviation professionals. Thereby, generate required aviation professionals for sustainable development of BD aviation industry.

Discussion and Results

A large number of skilled manpower are necessary for effective operations, management, and smooth operation. Based on the nature of functions, the aviation professionals have been divided into 02 broad categories- Operational professionals (OP) and Back Office Professional (BP) or Non-Operational professional. (Rabbani, 2023).

Table 1: Categories of Aviation Professionals

Operational Professionals (OP)	**Back Office Professionals (BP) or Non-Operational Professionals**
• Pilot • Cabin Crews • AME & Mechanics • Air Traffic Controllers • Regulatory • Aviation Safety and Security Personnel • Dispatchers • Ground Handling personnel • Air Cargo Managers • Operational Managers • Search and Rescue Manager • Aviation Medicine Specialists • Aviation Management Staffs	• Operational Air Transport Economics Marketing • Route Analysis • Aero politics • Ticketing and Reservation • Aircraft leasing • Human Resources Management • Finance • Customer Service • Insurance & Legal Affairs • Aviation Planning & Forecast • Research and Development • Airlines Distribution • Aviation and Environment etc.

Source: Rabbani, 2023

Demand of Skilled Manpower

"Current passenger trends in air transport in the Asia-Pacific region could be double to 8.2 billion in 2037." A 3.5% Compound Annual Growth Rate (CAGR) is predicted for the next 20 years, which will result in a doubling of passengers, according to the prediction. In Asia-Pacific, 46.7 million jobs and $944 billion in economic activity were supported by air travel. This equates to 2.5% of all employment and 3.1% of all GDP in Asia-Pacific nations in 2018 (IATA website, 2018). By 2036, 10 million people are anticipated to work in the aviation sector, including 620,000 pilots (for aircraft with more than 100 seats, 67 new pilots are hired every day), 125,000 air traffic controllers (13 new controllers are hired every day), 620,000 ground handlers, travel agents, supply chain logisticians, commercial service providers, security apparatuses, etc. There are 10 fields to study in aviation like Aerospace engineering, Air Traffic Controllers, Aircraft maintenance, Aviation management, Aviation safety, Cabin crew, Pilot training, Flight instruction, Aviation transport (Joanna Hughes, 2019).

Pilot and AME. Due to acute shortage of skilled pilot and AME, BD airlines have to invest a significant amount of money to hire AME and pilot from abroad. As there is growing need for additional aircraft, the demand of trained pilots, AMEs, technicians, and other flight and ground staff further increased. (Ahmed, 2023). There are 40 out of 400 active pilots and 30 out of 750 AMEs are foreigners (Mia, 2023).

Aviation Safety, Security and Regulations Expert. Safety is the top priority in the aviation industry. One needs a thorough understanding of aviation regulations, technical know-how, infrastructure, and a host of other IATA-mandated requirements to work in the airline industry. For an airline to operate effectively, qualified staff who are familiar with civil aviation rules, regulations, and standards are especially important. Most airline employees lack the necessary knowledge of aviation laws and regulations. Many airlines are unable to meet the conditions set forth by the civil aviation regulatory body (Shamsuzzahan, 2023).

Aviation Management Staff. There is currently a shortage of trained aviation management employees in BD's commercial airlines. Majority

of aviation management experts are trained and qualified in general management. Some of these businesses even depend on foreign workers to support and run them effectively (Rahman, 2018).

Qualified Operational Manager. Both commercial and state-owned aviation establishments lacked a qualified operational manager. On the other hand, a variety of aviation training institutions provide many operational management courses that are specifically geared towards the aviation industry. The lack of competent operational managers in BD is filled by staffs with aviation experience (Hussain, 2021). Many commercial airlines don't have qualified operational managers handling their operational planning. (Asif, 2023).

Air Cargo Manager. Enormous amount of air cargo is ready waiting for shipment in the HSIA cargo terminal. To manage air freight handling effectively, thorough knowledge and education are crucial. Though, there are a lot of opportunities with growing trend globally but BD hasn't expanded outside the domestic market yet. Properly educated and skilled cargo management personnel will contribute exponentially in our aviation industry's growth (Asif, 2023).

Search and Rescue Management Expert. Search and Rescue (SAR) of aviation accidents and incidents within BD airspace is vested on BAF. Though BAF has acquired modern SAR helicopter with maritime capability but lacks on formal joint training with civil airliners. Individual airlines generally maintains their well-trained flight safety personnel but lacks on joint training with BAF to meet the crisis. (Shamsuzzahan, 2023). Therefore, with the increase of aviation activities in BD, experts in SAR management are foremost for our aviation industry. (Miah, 2023).

Aviation Medicine Specialist. Aircrew and passengers are occasionally exposed to the peculiar aviation environment. While maintaining awareness of the physiological impacts of flying at high altitude and other factors, cabin personnel frequently need to provide necessary medical services onboard. There is no qualified aero-medical professionals or flight surgeon in airlines, except in BAF. There is a severe lack of knowledge in this aspects. Aero-medical specialists are required in every airlines, including more than one regulating body. (Miah, 2023).

Air Space and Traffic Manager. Only two institutions currently offer ATC professionals training, CAA and BAF. At both military and civil airports, CAA and BAF trained professionals are positioned as ATCO and assistant. However, their professional credentials sometimes lack or progress further due to academic endorsement from ICAO or CAAB. CAAB approved curriculum of BAF or private institutes under Aviation University can contribute enormously. (Rabbani, 2023)

Compliance Requirement in CAAB Approved Training

BATC is the only organization with EASA Part-147 approved training for AME licensing (Hussain, 2021). PART M is an airworthiness requirement for an organisation's administrative approval to continue air operations. In essence, any airliner must meet all the requirements as indicated in PART M of Air Navigation Order (ANO). The rule governing the approval of maintenance training organisations is found in ANO (AW) Part-147. ANO (AW) Part 147 is a national variant-specific adoption of EASA Part 147. Part-66 provides comprehensive guidance on the current AME licencing requirements. Recently, BSMRAAU has introduced AME certification for the graduates with incorporation of EASA Part-147 and Part-66 of CAAB (Habib, 2023). Therefore, the areas of demand and compliance requirement for skilled manpower in BD aviation industry are narrated clearly.

Case Studies on Successful UIC

Here four international aviation institutions in various areas are being studied for supported and targeted groups.

Case Study 1

Embry–Riddle Aeronautical University (ERAU), USA. ERAU, one of the largest and oldest university on aviation and aerospace is known as "Harvard of the Skies." This university offers more than 60 degree programmes of bachelor's, master's, doctorates, and other professional degrees. ERAU offers master's degrees in human factors, aerospace engineering, aeronautical science, and space education etc which are accredited by the Aviation Accreditation Board International and cerfied

by FAA (ERAU, 2023). University programme is formulated closely align with industry requirements, enabling students to readily adapt to market demands. Additionally, students have the chance to pursue advanced studies or engage in research endeavors that contribute to the industry's advancement. Consequently, the institution has emerged as a central focus for aviation professional training, equipping individuals not only for national but also global aviation endeavors.

Case Study 2

Singapore Aviation Academy (SAA). SAA is a Training Centre of Excellence (Platinum) Member of ICAO offers more than 110 courses over 33 areas. Besides regular programmes SAA also offers diploma in the following areas which are accredited with CAAS (SAA, 2023):

Table 2: Diploma Programmes Offered by SAA

Name of the Diploma	Area	Duration
Diploma in Civil Aviation Security management	It covers policy and operational considerations to address issues relating to Aviation security, ATC, ASBU, Safety management etc. Perspectives and interactions between various players and to prepare as an aviation executive with safety oversight and management systems in civil aviation. In addition, key safety consideration to meet national and organisational safety obligation.	06 weeks
Aviation Security Management Programme		3 days
Air Traffic Management Safety Investigation and Analysis		5 days
Methodology and Best Practices for Aviation System Block Upgrades (ASBU) Implementation		5 days
Diploma in Aviation Safety Management		weeks
Safety Management Systems Implementation		05 days
Safety Programme Implementation		05 days
Integrated Safety Management Systems		10 days
Source: SAA, 2023		

Case Study 3: Concordia University

Various courses, support organization and targeted group of this university are mentioned in the followings:

Table 3: Courses Offered by Concordia University

Ser	Name of the Course	Support Organization	Targeted Group
01.	AVSEC Professional Management Course	It was created in collaboration with ICAO	Aviation Security Professionals
02.	Management Certificate in Civil Aviation (MCCA)	It was offered in partnership with ICAO	Aviation management qualified personnel in civil aviation community
03.	Airport Executive Leadership Program	The Airports Council International (ACI)	Future CEOs, Deputy CEOs, VPs of airline operators

Case Study 4: University of Waterloo

University of Waterloo has the largest university-level aviation programme in Canada. The university's strength in science, environment, geomatics, and technology, along with training from one of the top-flight schools in the country, prepares the students for outstanding careers in the aviation and aerospace industries. Waterloo University has the following programmes:

Table 4: Programmes Offered by Waterloo University		
Name of Programmes	**Supported Programmes**	**Collaboration**
Geography and Aviation Bachelor of Environmental Studies (BES)	In addition, students receives in flight training with Preparatory Ground Instruction (PGI), and professional pilot theory courses. Upon completion, students are possessed for CPL and Multi-Engine Instrument Rating to become Canadian transport pilot.	Flight training is conducted with WWFC is considered to be one of the top flight schools in Canada. The flight centre has a large group of qualified flight instructors, and operates a fleet of 29 aircraft. In four years (205+ hours of total flight time).
Science and Aviation Bachelor of Science (BSc)		

UIC aspects BSMRAAU and BD Aviation Industry (from Case Studies)

All four universities accredited those programmes with their national CAA. BSMRAAU can create effective UIC, aligning following programmes as per aviation industry's requirement with valid CAAB accreditation or certification:

BSMRAAU can design programmes closely align with industry requirements, enabling students to readily adapt to market demands. Additionally, create chances for the students to pursue advanced studies or engage in research that contribute to the industry's advancement.

BSMRAAU can conduct readily available short duration programmes of SAA as handy reference. It will require CAAB acrredition and UGC approval (Fakhrul, 2023). Obviously, these will meet the requirement of skilled manpower not only for BD but also for global aviation industry.

BSMRAAU can conduct various ICAO/CAAB supported programmes designed for higher level professionals like CEO/CFO/Mangers of aviation industry with appropriate approval from CAAB, would meet the requirement of high level skilled manpower.

BSMRAAU can conduct CPL with Multi-Engine Instrument rated transport pilots in additon to Bachelor degree which requires CAAB accredition. It is to be supported with Civil Flying Club or Flying Instructor School (FIS) or BAFA. This programmes will meet the acute shortage of pilots requirements.

BSMRAAU should maintain a central focus for aviation professional training, equipping individuals not only for national but also global aviation endeavors. BSMRAAU should take following steps simultaneously:

First step is to utilise diverse and dispersed resources and facilities with BSMRAAU as hub including credible academicians. Consequently, support from various organisations would facilitate programmes to make all related trainings. (Khan, 2023)

By launching a variety of programmes, BSMRAAU can gradually address all segments of both types of Next Generations Aviation Personnels (NGAPs). BSMRAAU needs to have strong infrastructures with enough financing, as well as wholehearted support from BAF and BD government. (Fakhrul, 2023)

Therefore, necessary lessons are drawn for the BSMRAAU, BD aviation industry and CAAB to assist in developing a formidable UIC plan.

Areas of UIC Alignment

BSMRAA started with 07 departments in 04 faculties of aviation and aerospace engineering and managements to create aviation professionals,. Its faculty expansion is spread over two decades, targets to open up 07 faculties. From 2024 onwards, BSMRAAU will be able to provide qualified graduates for employment in various area of aviation sector. On 28 February 2019, BD National Parliament has passed Law No. 05 of 2019 and was published as BD Gadget on the same date. As per para 05 of this Gadget, BSMRAAU is authorized to affiliate with all aviation academy, institute, college, center and education institution of BD with appropriate administrative circular. (Habib, 2023). As per para 06 of BD Gadget of

Law (No. 05 of 2019) and UGC order, BSMRAAU has been empowered broadly with 31 aspects. These major aspects of these empowerment would assist BSMRAAU for effective collaboration or affiliation with the all aviation institutes, academy, training center and colleges etc of BD. (Habib, 2023). As a mediator and authorising authority, CAAB has a significant role to play in fostering cooperation. Instead of choosing professionals with backgrounds in physics, math, or general engineering, CAAB may choose them from BSMRAAU graduates. CAAB must set up the environment and make it simpler for recent graduates to enter the aviation sector. Holistic approach needs to be borne about aviation industry, to make effective collaboration with BSMRAAU at all levels of skilled professionals' development and appropriate utilization.

Creating Skilled Aviation Professionals in BD Presently, following 07 aviation academies are generating aviation professionals in BD:

Table 5: Aviation academies creating skilled aviation professionals in BD

Ser	Training Institutes	Type of the Organization
01	Civil Aviation Academy (CAA)	Training Academy of CAAB
02	Bangladesh Airlines Training Center (BATC)	Approved 147 maintenance training organization
03	Bangladesh Flying Academy and General Aviation Limited (BFA&GA)	Approved Flying training organization
04	Galaxy Aviation Academy (GAA)	Approved Flying training organization
05	Arirang Flying School (AFS)*	Approved Flying training organization
06	Airmen Training Institute (ATI)	Approved 147 maintenance training organization
07	BSMRAAU	Aviation Public University
N.B. * At present Arirang Flying School is not operating.		
Source: Rabbani, 2023		

UIC Alignment of the Demand Areas

Table 6: UIC (BSMRAAU and Aviation Industry) Alignment of the Demand Areas

Demand Areas	UIC Aspects	Support Organisation
Commercial type rated Pilot	BSMRAAU may conduct CPL with Multi-Engine Instrument rated transport pilots in additon to BSc on Science and Aviation (University of Waterloo)	BFA&GA, GAA, AFS, FIS and BAFA
Type rated AME	BSMRAAU starting CAAB approved AME certification with Bachelor degree from 2024	BSMRAAU
Aviation Management Staff	Master's programme in Aviation Management has been conducting in BSMRAAU	BSMRAAU
Aviation Safety, Security and Regulations Expert	Diploma in Civil Aviation Security management (06 weeks), Aviation Security Management Programme (03 days), Diploma in Aviation Safety Management (06 weeks), Safety Management Systems and Safety Programme Implementation (05 days), Integrated Safety Management Systems (10 days) and AVSEC Professional Management	BSMRAAU may conduct short courses with CAAB accreditation and UGC approval in support of FSI and AVSEC
Operational Manager	Management Certificate in Civil Aviation (MCCA) and Airport Executive Leadership Programme	

Table 6: UIC (BSMRAAU and Aviation Industry) Alignment of the Demand Areas		
Demand Areas	**UIC Aspects**	**Support Organisation**
Air Cargo Manager	Conduct formal short training to generate adequate Air cargo manager of international standard from Private aviation training centre/institutes	BSMRAAU affiliated with Private Institute
Search and Rescue Management Expert	Formal joint training on SAR between airline operators and BAF in AW-139 MSAR, Bell-212 and Mi-17 helicopters to meet the crisis. There may be refresher training periodically	BSMRAAU affiliated with 9, 31 Squadron and 109 MSAR (U)
Aviation Medicine Specialist	Conduct formal short training to generate adequate Air cargo manager of international standard	BSMRAAU affiliated with BAF AMI
Air Space and Traffic Manager	Air Traffic Management Safety Investigation and Analysis	BSMRAAU affiliated with CAA & ATS

Major Challenges to UIC

BSMRAAU faces a numerous major challenges for UIC in support of BD aviation industry are:

Difference in Culture and Management Alignment. Existing cultural norms, management's vision, and the objectives of BSMRAAU and aviation industry extremely differs which appears to be a barrier for UIC (Khan, 2023). Academia focuses on fundamental research, knowledge sharing, technical solutions in pursuit of a problem, patent, theory etc. Whereas, industry is focused on commercial standpoint and client concerns (Fakhrul, 2023).

Lack of Funds and Entrepreneurship. Due to budgetary constraints and lack of funds, expert professors of aviation fields can't be employed. In general, honourium requirement for international Professor/Instructor is higher (300 ~ 500 USD) with the allotted budget (50 USD) which BSMRAAU is unable to manage. Due to tough policy with rules and regulations entrepreneurs get discouraged to contribute in university or faculty for talent-hunt, competency development (Fakhrul, 2023). There may be MOU between BATC and US-Bangla Ailines in various terms as entrepreneurship with CAAB support in easing of rules and regulations (Khan, 2023).

Intellectual Property Rights. Rights to intellectual property concerns frequently overlap with other issues, like project management and incentives. Most of the time university or individual aggressively deny to share the patent and licence of their inventions (Khan, 2023).

Lack of Experienced Faculty on Aviation Management. BSMRAAU has been suffering for inadequate qualified and experienced Professor/ Lecturer in various aviation field of study. Moreso, due to multiple number of trainees and engagement in different publications, available lecturer gets lesser time to contribute. As hiring foreign professor is too costly in terms of provided budget and honorium (Fakhrul, 2023).

Institutional Incentives. University and commercial sector incentive structures might not acknowledge or reward the crucial contributions. Huge difference in levels of incentives in two stakeholders discourages UIC. (Khan, 2023)

Challenges to BSMRAAU-Airline Collaboration. Major challenges are the airlines frequently view academia as an adversary because of their business motivations. As airlines place an excessive amount of emphasis on operations, whereas university-run programmes are mostly theoretical. As a result, university is lagging behind the inventiveness and need for new ideas in business. Due to lack of EASA Part-147 approved AME training organisation, only BATC generates AME certified engineers. Thereby, airlines hires foreign engineers for their companies and drains BD aviation profits to them (Hussain, 2021).

Challenges to BSMRAAU-CAAB Collaboration. CAAB has sacred responsibility to assist in formulation and approval of relevant policy to facilitates the UIC programmes and affiliated part of national gadget 28 February 2019 (Habib, 2023). Again, easier policy, rules and regulations would bring airline magnets to invest in our aviation industry. Thereby, collaboration between the BSMRAAU and CAAB is very crucial and time-sensitive. (Fakhrul, 2023). CAAB, has plays significant role for the management of airports, air traffic, and aviation security due to constant audit of ICAO. To help states realising ICAO strategic objectives, CAAB is the legally authoritative certifier for different categories of skill competence in aviation-related employment. Moreso, ICAO-sponsored research dissemination throughout aviation industry is another prime requirement (Hussain, 2021).

Challenges to BSMRAAU-BAF Collaboration. BSMRAAU owes a great deal to BAF for its assistance in providing professionals for administrative and financial support including academicians since beginning. BSMRAAU extensively uses BAF's maintenance and training facilities for their students' practical classes. Moreover, faculty members are mostly from BAF expertise in their arena to provide the most recent scientific and technological subjects, particularly aerodynamics, aero-engine, navigation, meteorology, avionics and electronics, space system, and aerospace power (Fakhrul, 2023).

Mitigation through a Formidable UIC Plan

Through several UIC improvement initiatives, main stakeholders are industry (Airline operators), regulator (CAAB), and university (BSMRAAU). "The Trinity of Partnership" develop a unified capability to solve difficulties and chart a course forward. UIC's true nature encourages us to work together rather than compete. The formidable UIC model is developed with three significant broad aspects, period of 06 years each. These are as follows:

- Capability development (Short-term, between 2024-2029).
- Affiliation at home and abroad (Mid-term, between 2030-2035).
- Sustainable development of Aviation industry (Long term, 2036-2041).

Capability Development (Short-term, between 2024-2029). In this short-term phase, main focus to be given in capability development and the major tasks are:

- Prepare and update the syllabus of different faculties/departments in line with CAAB/ICAO/EASA approved programme and attain accreditation subsequently.
- Regular arrangement of experienced international professor on various important programmes/faculties.
- Establish MOU with different airline operators enabling internship on industrial training from 3rd year onwards and expedite employment process for the graduates.
- Make special MOU for yearly employment (may be best 10~15 graduates on merit based) of graduates with various private airlines
- Develop continuous fund generation from government, VC's fund, donor organisations, or CSR funds of different business groups.
- Take-up various R&D project on current industrial problems of BD aviation industry.
- Conduct of various Seminar, workshop, symposia etc with local and international aviation experts.
- Simplified and accessible short-term programme for both operational and non-operational professionals with valid CAAB accreditation. Accordingly, develop policies in conjunction with BAF, CAAB, and UGC.
- Development of required training facilities for AME, cabin crews and ATCOs including simulators.

- Creation of more aviation training facilitaties to provide non-operational programmes like aviation law, finance, human resources, leasing, insurance, etc.
- Government support may be provided in terms of funds for R&D, PhD and Foreign & local expertise management, Labs & Simulators procurements and Infrastructure development etc.
- Implementation of evidence and competency-based training for engineering and maintenance.
- Inclusion of human resource planning tools, accredited training and educational programmes adapted to the aviation industry for next generation.
- Formalize working group consisting of representatives from industries, education, training providers and regulatory body.

Affiliation at Home and Abroad (Mid-term, between 2030-2035). In this mid-term phase, main focus to be given for affiliation of BSMRAAU with various aviation institute, college, training centre as per national gadget 2019 (Law No. 05, 28 February 2019) with other major tasks:

- Public and private owned aviation training institute and centre should be gradually affiliated as per BD gadgets (Law No. 05, 28 February 2019).
- Affiliation with 208/210/214/216 MROUs to develop expertise and capacity building. 208 MROU is certified to overhaul Bell helicopters, private companies operating Bell helicopters may take the support.
- BSMRAAU TO&E may be revised to create vacancies for aviation industry experts.
- BSMRAAU faculty's visit to aviation industry for ascertaining gaps between theory and realities. Joint research may be conducted involving faculty and industry experts.

- Industry may provide fund to selected students for higher studies on industrial problems. Scholarship in collaboration with aviation industries for higher education.
- Regulatory body (CAAB/ICAO) may be briefed adequately for Government support to BSMRAAU training.
- Collaborations amongst various academies of BD as well as foreign countries of this region like - Singapore, Canada, Hong Kong and Republic of Korea etc.

Sustainable Development of Aviation Industry (Long term, 2036-2041) In this long-term phase, main focus to be given in policy development and generation of adequate skilled manpower for BD aviation industry. Better awareness on industry's practice and CAAB requirements to be focused continuously and update regularly, with the major tasks are:

- Prepare and gain approval of aviation friendly policies to encourage aviation giants to invest.
- Articulation and approval of appropriate policy, rules and regulations for sustainable development of aviation industry consulting all stakeholders.
- Invite successful entrepreneurs and top management to exploit the opportunities in funding the big projects of industry's requirement with benefit sharing
- Knowledge and skills up-gradation with research projects and innovation encouragement etc. Subsequently, implementation of ideas into viable products or solution.
- Collaboration with foreign renowned aircraft/helicopter industries to enhance credibility such as joint R&D, aircraft/helicopter manufacture infrastructure etc.

Conclusion

BSMRAAU faces acute shortage of fund, qualified world re-known academicians and affiliations with local and international institute and universities (Fakhrul, 2023). Present cultures of the two organisations' managements are not aligned and diverge, and these are the main obstacles to have collaboration Airlines, CAAB, and BAF. As first step, BSMRAAU should utilise diverse and dispersed resources and facilities as hub with credible academicians. Consequently, support from various organisations would facilitate the programmes to make all related trainings. By launching a variety of programmes, BSMRAAU can gradually address all segments of both types of NGAPs. BSMRAAU needs to have strong infrastructures with enough financing, as well as wholehearted support from BAF and BD government. BSMRAAU can create UIC with appropriate approval from CAAB at least in 09 areas. In assistance with at least 07 public and private aviation training institute to contribute directly to BD aviation industry. Moreover, BD Gadget authorized BSMRAAU to affiliate with 31 aviation related academy, college, center and institution of BD with governmental support to conduct various courses to develop skilled aviation manpower.

BSMRAAU can create effective UIC while aligning programmes with aviation industry's requirement and CAAB certification to enable students quickly adapt to market demands. Additionally, create chances for the students to pursue advanced studies or engage in research that contribute to the industry's advancement. BSMRAAU can conduct short duration programmes following SAA which requires CAAB acrredition and UGC approval. Also conduct various ICAO/CAAB supported programmes designed for CEO/CFO/Mangers like Concordia University to meet their requirement. Moreover, conduct CPL of transport pilots programme with Bachelor degree to meet the acute shortage of pilots requirements with CAAB accredition and supported by Civil Flying Club or Flying Instructor School (FIS) or BAFA. A formidable UIC model is developed with three significant broad aspects, period of 06 years each. These are Capability development (Short-term, between 2024-2029), Affiliation at home and

abroad (Mid-term, between 2030-2035) and Sustainable development of Aviation industry (Long term, 2036-2041). With all these UIC plan, BSMRAAU focusing for aviation professional training, equipping individuals not only for BD but also global aviation endeavors.

References

1. ASM Fakhrul., 2023. Vice-Chancellor, BSMRAAU, 27 April 2023.
2. Rahman, M. H., 2023. Pro-VC, BSMRAAU, 24 June 2023.
3. Faroque, M., 2023. Planning & Project Director, BSMRAAU, 24 June 2023.
4. Hasan, A. Z. M, 2023. Head of Department, Aviation Safety Management Department, BSMRAAU, 24 June 2023.
5. Alam, M. J, 2023. Head of Department, Aeronautics Enngineering Department, BSMRAAU, 24 June 2023.
6. Rahman, M. R, 2023. Head of Department, Avionics Enngineering Department, BSMRAAU, 24 June 2023.
7. Ahmed, M.K., 2023. Member, Flight Safety & Regulation, CAAB, 25 April 2023.
8. Miah, M.M.A., 2023. Director, Flight Safety & Regulation, CAAB, 25 April 2023.
9. Rabbani, M. G., 2023. Senior Executive, Law department, Flight Safety & Regulation, CAAB, 25 April 2023.
10. Mannafi, A. S. M., 2023. Member, Aviation Security, CAAB, 02 July 2023.
11. Rahmatullah, C. M. S.,2023. Head of AIG-BD,CAAB, 25 April 2023.
12. Khan, M. J., 2023. Director Planning, Biman Bangladesh Airlines, 25 April 2023.

13. Ahmed, Gulger., 2023. DFO, Mehgna Aviation Airlines Limited, 10 June 2023.

14. Asif, Imran., 2023. CEO, Air Astra Airlines, 11 June 2023.

15. Zahan, A. A. S, 2023. Head of Safety & Captain, US-Bangla Airlines Ltd, 01 July 2023.

16. https://www.academiccourses.com/articles/10-fields-to-study-in-aviation [Accessed 08 Mar. 2023]

17. https://www.bsmraau.edu.bd/programs. [Accessed 10 Mar. 2023].

18. https://bdnews24.com/business/ejk3pbvhmh [Accessed 10 Mar. 2023]

19. https://businesspostbd.com/national/aviation-sector-growth-will-triple-in-next-15-years-state-minister-30061 [Accessed 10 Mar. 2023].

20. https://erau.edu/ [Accessed 10 May 2023].

21. https://caab.portal.gov.bd/ [Accessed 22 April 2023].

22. http://www.ugc.gov.bd/en [Accessed 05 July 2023].

23. https://www.caas.gov.sg/saa [Accessed 15 June 2023].

24. https://www.concordia.ca/jmsb/executive-education/programs/aviation.html [Accessed 23 June 2023].

25. https://uwaterloo.ca/aviation/flight-training [Accessed 15 June 2023].

26. Hussain. M (2021). Industry-University partnership towards development of aviation industry in Bangladesh: Challenges and way forward.

27. Khan, M. J. (2021) Sustainable Development of Aviation Industry in Bangladesh: Status and Emergence of Industry-University Collaboration.

28. Rabbani, S. M. G. (2021) Development of skilled aviation professionals in Bangladesh: Necessity, constraints, and viable future measures.

Author

Group Captain Sk Ashraful Hossain, afwc, psc, GD(P) has been serving in BAF for last twenty six years. He was commissioned on 29 June 1997 with 34 GD(P) course in the General Duty (Pilot) branch. He is a category 'B' Flying Instructor and Fighter Category 'B' operational pilot. He has attended all related basic and advanced flying and ground training courses at home and abroad. In his career, he has served in 11, 15, 21, 25 and 35 Squadron as Flying Instructor and Flight Commanders. He has commanded successfully 25 Squadron (Fighter Training) and Recruit Training School of BAF. He has served as Deputy Director (Grade-1) in the Directorate of Recruitment, Flight Safety, Administrative Co-ordination and Chief Inspector's branch of Air HQ. He has served as Flight Inspector in BANIAR-6 and as G-5 of Norther Sector of MONUSCO. Group Captain Sk Ashraful Hossain is a graduate of Aeronautics from National University. His post-graduations include MDS in Defense Studies from BUP. He is a certified Instructor by CAAB in Safety Programme Management (SPM) and completed executive training in Human Factor analysis from CAAB. He has been awarded with COAS Commendation for extra-ordinary performance during the pioneer deployment of F-7BGI fighter aircraft from China to Bangladesh. He has completed Armed Forces War Course 2023 in NDC, Mirpur.

NDC JOURNAL
Security Through Knowledge

AN ANALYSIS OF THE COMMAND AND CONTROL SYSTEM FOLLOWING THE TRANSITION OF LEADERSHIP FROM "GENERATION X" TO "GENERATION Z": BANGLADESH ARMED FORCES PERSPECTIVE

Colonel S M Moniruzzaman, SGP, afwc, psc

Introduction

Two generations in the Bangladesh Armed Forces are now coexisting, as with every other military worldwide. 'Generation X' members were born in the analog era and substantially served in the Armed Forces before the Armed Forces transitioned to the digital era. The members of 'Generation Z' (also known as iGeneration) are individuals born into the digital age and have no prior exposure to the analog one (Twenge, 2018). It is close enough when Generation Z will ascend to Armed Forces' command. According to a basic estimate, Generation Z will command the entire Armed Forces in about twenty five years. Modern technology and digitalization are also expected to advance far away within this quarter-century. With the development of technology and digitalization, a shift in the command and control system of the Bangladesh Armed Forces is inevitable. As technology develops, it is anticipated that the Bangladesh Armed Forces will acquire superior intelligence, surveillance, and reconnaissance (ISR) capabilities and advanced communication technologies, significantly altering the decision-making process. Machines may replace the use of human soldiers in hazardous tasks. Decisions about administration and logistics are expected to change because of the widespread use of contemporary technology, automation, and computerization. As a result of technological development, the command and control systems might undergo numerous other transformations. The question is whether Generation Z military leaders will benefit more from the revamped command and control system.

It is difficult to say precisely what stage the development of modern technology and digitalization development will reach in the next twenty five years. Nevertheless, the evolution of command and control of the Bangladesh Armed Forces will largely depend not only on transformations in technology but also on changes in the socio-economic conditions of Bangladesh. So, to analyze what kind of command and control system they will experience when Generation Z commands the Bangladesh Armed Forces, it is necessary to study what kind of socio-economic and technological changes Bangladesh may experience in the next twenty five years.

This article has first done some research on the potential socio-economic and technological transformations that could take place in Bangladesh over the next twenty years to examine what the command and control system might look like and how effective it would be during Generation Z. The analysis is then conducted to determine what modifications to the command and control system the existing Armed Forces might come across in the changing environment. The effectiveness of the command and control system for Generation Z is then illustrated through a critical analysis. The potential challenges of the upcoming command and control system are discussed, along with the Bangladesh Armed Forces' ways of overcoming them.

Literature Review

Researches have been done all across the world to determine how the command environment will change as generations progress. According to (Wachowiak 2024), the capacity for innovation and creativity among military units is one of the main advantages that result from generational diversity. He asserts that every generation contributes a distinct viewpoint and life experience that might inspire creative problem-solving approaches. Conversely, (Steve 2016) stated that although the requirements of different generations may differ, there appear to be more similarities than differences. He argued that because the area has its own culture and opinions are more

consistent throughout generations, these discrepancies are further reduced when it comes to military enlistment and commissioning. However, a comprehensive study into how command and control systems change with generational shifts in the context of the Bangladesh Armed Forces remains to be done.

Research Methodology

A mixed-method approach has been adopted to conduct a descriptive research. Content analyses were the primary approach used for obtaining data. Besides, few senior officers have been interviewed along with focus group discussions with the junior officers.

What are Generation X and Generation Z?

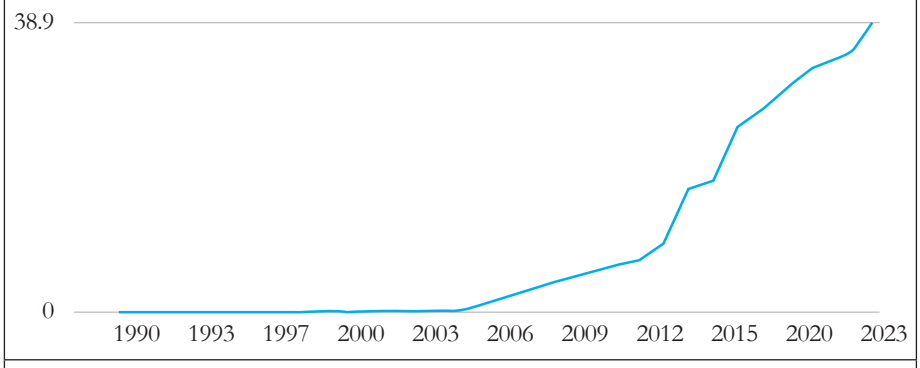
The media and popular parlance have defined several generations based on the birth period, despite the fact that no official commission or body decides the titles of the generations. "Generation X" are those who were born between 1965 and 1980. The Bangladesh Armed Forces' Generation X members have served for at least 23 years and are currently in senior leadership positions at various levels. Up to the years 2004–2005, people of Generation X in Bangladesh had several decades of analog experience before moving into the digital era (The Global Economy, 2020). Sometimes referred to as "Generation Y" or Millennials, those born between 1981 and 1994 are frequently lumped in with Generation Z. This generation's Armed Forces members range in service age from 10 to 22, and they currently occupy mid-career and junior leadership roles. "Generation Z," or those born between 1995 and 2012, are sometimes called the "iGeneration." Generation Z members are still enlisting in the Armed Forces and have served a maximum of ten years. Members of this generation, born in the digital age, will be assigned command of the entire Bangladesh Armed Forces over the next twenty five years.

Expected Socio-Economic and Technological Transformations in Bangladesh over the Next Twenty Five Years

Bangladesh is now the 35th country on the list of nations with a GDP of USD 460.8 billion (The Dhaka Tribune, 2023). According to PricewaterhouseCoopers (PwC), Bangladesh will have the world's 28th-largest economy by 2030 and has the potential to overtake the 23rd-largest economy by 2050 (The Daily Star, 2018). A growing labor force of working age, growth in human capital, expansion in physical capital, and factor productivity would be the four main driving forces behind the growth, according to PwC. Nevertheless, this advancement depends on good governance, political stability, and developing institutions that promote growth.

Bangladesh is anticipated to make technological advancements as its economy grows. It's technological vision declared, "Five G (5G) will be on the run within 2025. Future technologies like artificial intelligence (AI), robotics, big data, blockchain, and IoT will be widespread" (National Strategy for AI, 2020). Every village in the nation will be connected by fiber optical cable by 2025, according to the Information and Communication Technology (ICT) Ministry's plan to bring high-speed internet to rural areas (The Business Standard, 2022). As of January 2024, 44.5% of Bangladesh's population uses internet services; this number is expected to peak in the next quarter as internet access spreads across more rural areas (Kemp, 2024). As a result of the expansion of high-speed internet connectivity in rural and remote areas, every member of the armed forces, from the highest headquarters to the lowest soldier, is likely always to have access to data connectivity.

Figure 1: Internet Usage in Bangladesh



Source: The GlobalEcomony.com

In robotics, Bangladesh's strategy focuses on developing the country's competitiveness, human resource development, research and development (R&D) and innovation capabilities, robot production and maintenance capacity, and support for robotics start-ups (National Strategy for Robotics, 2020). Therefore, it is anticipated that robotics will be fairly used in Bangladesh military armaments such as unmanned ground and aerial vehicles (UGV & UAV), automatic weapon systems, heavy engineering equipment, and the devices used for combat reconnaissance and surveillance, search and rescue operations, mine laying and breeching, bomb disposal tasks, etc. Bangladesh also embraces AI to advance its economy and society by creating an AI innovation hub, formalizing its legal framework, developing data-driven policies, and preparing its workforce (National Strategy for AI, 2020). The Bangladesh Armed Forces are also likely to integrate AI in decision-making, data processing and research, battle simulation, target identification, cyber security, transportation, casualty care and evacuation, and other areas. To support the growth of the local economy and raise the standard of living for the populace, the Bangladesh Government also places a strong emphasis on the Internet of Things (IoT) education, the development of skilled human resources in IoT, and the application of IoT at all levels of state and society (National Internet of Things Strategy, 2020). The Bangladesh Armed Forces would also work to use IoT best in several areas, including data collection on the

battlefield, troop health monitoring, equipment and vehicle maintenance, enemy identification, enabling smart cantonments, remote training, data analysis, and other areas.

Transformations in Bangladesh Armed Forces Command and Control System that Generation Z are Likely to Experience

It is often challenging for Generation X military leaders raised in the analog age to adapt to incorporating modern technologies. Many still regard the analog era as the golden age, even though they acknowledge the necessity of current technologies. On the other hand, because they were raised in the digital era, military leaders of Generation Z will be highly reliant on technology. Therefore, this generation of military leaders will completely embrace and attempt to utilize the advantages of emerging technological developments. Therefore, the functional components of command and control systems, including decision-making, communication, the employment of manpower, security, feedback, etc., would also undergo significant transformations due to technological progression. The following paragraphs lay out the expected evolution in the Armed Forces command and control system that Generation Z is likely to experience.

Decision Making at Tactical Level. In dealing with any crisis at the tactical level, decision-making responsibility is usually given to the ground commander. It is not practicable for higher commanders to completely visualize or comprehend the ground situation from their headquarters or to make judgments based on it, especially for the Bangladesh Armed Forces, due to insufficient ISR capabilities. As a result, the ground commander is always given the initiative to make decisions. However, as the ISR system advances, commanders at operational and even strategic levels will be able to make comprehensive decisions while positioned in their headquarters, assisted by computers, after visualizing the ground situation using cameras on the soldiers' helmets, drones flying above them, and satellite videography from higher positions, etc. In that circumstance,

the headquarters can make a more prudent decision regarding the tactical situation. However, it is possible that the ground commander's initiative would be curbed in that circumstance.

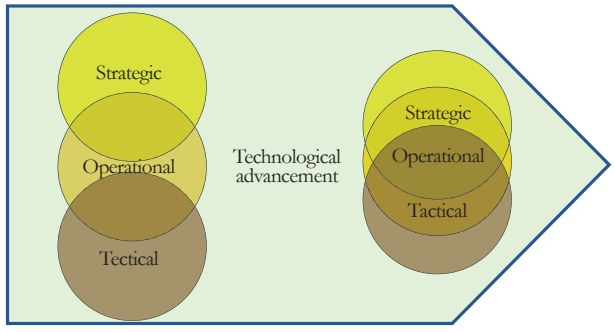
Curbing Risk to Soldiers' Lives. The Bangladesh Armed Forces' extensive employment of UAVs and UGVs in the approaching technologies will likely reduce the risk to troops' lives on the battlefield. Additionally, the risk posed by human soldiers will be reduced through the use of autonomous mine sweepers, bomb disposal robots, bulletproof clothing, and counter rockets, artillery and mortars (C-RAM), etc. This will probably make it easier for tactical commanders to deploy their troops even in the most hazardous spots on the battlefield.

Effective Employment of Manpower. The world's armed forces are changing following the modern military's increasing automation. Most countries are considering reducing their military size to match their substantial investments in new technologies (Daphne, 2021). However, the Bangladesh Armed Forces might be unable to apply the same approach. Despite significant investments in technological advancement, the Bangladesh Armed Forces may still encounter challenges with reducing manpower due to the country's desire to expand employment opportunities to accommodate expected population growth. If this is the case, commanders at all levels might have challenges employing the workforce effectively.

Freedom of Employing Troops. Modern technology can be incorporated into warfare systems, including weapons, sensors, navigation, air support, and surveillance, to improve performance and reduce reliance on human input. These systems need lesser maintenance due to their increased efficiency. Human error is reduced by eliminating the necessity for complete human control of warfare systems, and human capacity is freed up for other important activities. As a result, commanders at all levels will have the freedom when deciding how to use their troops without worrying about a shortage of manpower.

Communication. Communication is essential for military leaders to maintain command and control both on the battlefield and in peaceful locations. The goal of future military communications would be to facilitate reliable communication from anywhere to everywhere, from a ground soldier to the supreme commander, with the maximum speed and the least amount of latency by utilizing nodes placed underwater, on the surface of the water, on land, in air, and space. The gaps between military and commercial communications systems are anticipated to be reduced for Generation Z. The necessity for sending data such as maps, photos, and videos to the soldier deployed at the front line will further shift the requirements from voice communication to data communication. Future military communications equipment will likely be more band-covering, lighter in weight, smaller in size, and capable of carrying more voice and data. The new systems will require more interoperability, multimode operations, and enhanced spectrums. Thus, every soldier in the military may have a small portable communication device in the future that they can use to communicate voice and data from anywhere in Bangladesh. Each soldier's disposition and activity may also be learned through those devices. Military communication on the battlefield or during operations will not be restricted from headquarters to headquarters only; instead, the highest headquarters will be in direct communication with the soldier on the front lines. With the development of communication technology, the gaps between strategic, operational, and tactical levels of warfare are anticipated to decrease (Figure-2). As a result, information or decisions regarding any issue will be available rapidly. On the other hand, to ensure information security, commanders must put up much effort.

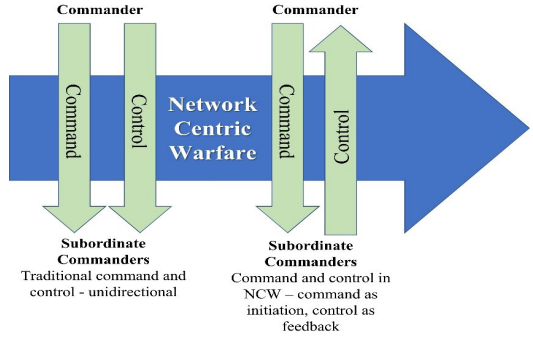
Figure 2: The levels of warfare with technological advancement



Source: Author's own creation

Network Centric Warfare (NCW). In NCW, the full scope of contemporary command and control technologies is envisioned. Modern technology would make it possible to further the combined arms approach. In fact, with the development of global communication and the advancement of high-precision and standoff weapons systems, all connected within the information domain, Generation Z commanders can synchronize operations in various domains while using various weapon systems in an ever-faster decision-making loop. However, a commander's potential engagement with nearly each of their subordinate units or even the soldiers may transform the commander's function from that of a coach who provides direction to his team to that of a chess player who has direct control over the pieces being played (Simonetti, 2020). The enhanced battlefield understanding offered by NCW would enable commanders to comprehend the battlefield considerably more precisely, quickly, and distantly. Technology would dramatically improve the certainty and accuracy of how combat is conducted. By stepping up purchases of sophisticated technology, Clausewitz's fog of war could be reduced. However, an upshot of this evolution could be a return to the conventional command and control strategy, where command and control would be viewed as unidirectional rather than a positive feedback loop. The micromanagement of warfare, for instance, which could harm mission command philosophy, is another potential risk linked with this development.

Figure 3: Command and Control functions in Network Centric Warfare



Source: Marine Corps University Journal, Volume 11, No 1, 01 November 2020

Understanding Subordinates' Psychology. Understanding a subordinate's psychological profile is crucial at all levels of command. Currently, commanders are using approaches for learning about the psychological characteristics of their subordinates through group or individual, formal or informal interactions, input from various sources, body language reading, evaluation of their individual or collective performances, etc. This approach will get more straightforward in the future as technology develops. The psychological profiles of the soldiers will be studied using various AI techniques. For example, each soldier may have a band or chip placed on his body through which a computer will automatically assess his psychological changes. This system would allow a commander to know how his troops have responded to his commands, state of current morale, and other details.

Critical Analysis of the Transformations in Command and Control System

Undoubtedly, Bangladesh will make significant technological progress over the next twenty five years compared to today, which will benefit the Armed Forces. Members of Generation Z will rise to various levels of command in the Armed Forces during the next twenty five years. These Generation Z commanders will encounter advantages and challenges in establishing

their command and control as technology develops. The most significant benefit they will experience is that all their supervisors and subordinates will be from Generation Z. Senior and mid-level commanders are currently from Generation X. In contrast, junior subordinates are from Generation Z. Because of this, when Generation X leaders currently command Generation Z personnel based on their concepts of analog and digital experiences, it naturally leads to a perception gap. This gap will likely eliminate when Generation Z is represented in every command position. The second benefit will be in decision-making for Generation Z commanders. It is anticipated that every decision at any stage can be made faster and with more precision than it now is because of the enormous advancements in communication technologies and the support of automation in decision-making. In addition, the NCW approach would offer operational and strategic level commanders the ability to precisely analyze tactical situations and make prudent decisions from a distance. The third benefit would be in terms of efficient use of manpower. Fewer individuals will accomplish more work due to automation and digitization in weaponry and equipment. A fourth significant benefit is that it would no longer be necessary to rely entirely on one's analysis to comprehend the psychology of subordinates. With the widespread use of AI, commanders are expected to know and understand the psychological aspects of subordinates through automated analysis.

On the other hand, technological innovation may stifle the initiative of young leaders in making tactical-level decisions. The network-centric decision-making process will probably encourage commanders at operational or even strategic levels to intervene with tactical decisions, reducing tactical commanders' initiatives. More robotics, AI, and automation in the military would once more eliminate much of the work done by the soldiers. For tactical-level commanders, effectively employing these additional soldiers may provide another obstacle. Threats to information technology and digital networks will multiply as digitalization progresses. The leaders of Generation Z will confront an enormous challenge in ensuring digital security.

Ways Forward for the Bangladesh Armed Forces to Take on the Forthcoming Challenges

Bangladesh Armed Forces will rapidly advance in digitalization over the next twenty five years. The use of military troops in many Armed Forces activities is anticipated to decline as technology develops. Nevertheless, considering Bangladesh's large population and employment problems, reducing the number of military personnel might not be appropriate. However, the military must consider how to use these extra personnel most effectively. Despite developing a network-centric command and control system, the system must offer tactical commanders the flexibility to make final decisions in tactical situations. Future cyber threats must be anticipated, and the Bangladesh Armed Forces must start preparing for them. A joint cyber command might be formed in the Armed Forces, with members of the three military services working with civilian cyber counterparts as the group's driving force. Armed Forces' cyber and technology policies should be developed so that modern digitalization supports and facilitates the armed forces' activities rather than inconveniencing the armed forces members.

Conclusion

At the senior and mid-level commands of the Bangladesh Armed Forces, members of Generation X are currently in command, whereas most of their subordinates are from Generation Z. Due to the rise of digitalization from 2004–2005, a synchronization gap naturally exists between these two generations. However, this disparity is expected to disappear within twenty five years after Generation Z leaders command every component of the Bangladesh Armed Forces. There is a possibility that the transformations in the command and control system that the commanders of Generation Z are likely to apply might take place as digitalization continues to advance.

According to the Bangladesh's digitization policy, fiber optic connections to every village in Bangladesh are pretty close. Then, any piece of land in

Bangladesh will have access to the internet, which will shortly be upgraded to 5G. Bangladesh has consolidated the vision of advancement in the other modern technology fields, such as AI, robotics, IoT, etc., which includes human resource development and elevation of maintenance capabilities through robotics, optimal use of AI and IoT in economic and social platforms, and so forth. In the areas of communication and connectivity, weapon systems, engineering, search and rescue operations, medical facilities, training, ISR, and many others, the Bangladesh Armed Forces will also benefit from this technological advancement. The synchronization gap would be eliminated in the realm of command and control of the Bangladesh Armed Forces. The decision-making process would be automated, made more superficial, and faster with AI, consistent connectivity, and communication between the soldier at the front lines and the highest headquarters. Robotics, AI, and connectivity would improve the utilization of unmanned platforms while lowering risks to human soldiers. In addition, using computerization and automated systems everywhere would save much labour and, to a certain extent, lessen the necessity for human soldiers. Maintaining constant communication between superiors and subordinates would be possible once the soldiers have access to contemporary IT and communication tools. Digitalization and automation would lead to the NCW, which would put the entire operational area under the command and control system of the highest headquarters. With the widespread application of AI, reading the psychology of subordinates might be made simpler for commanders at all levels, which would have enormous implications for the command and control system.

Nevertheless, there is concern that the initiative of the tactical commanders may be constrained if NCW and enhanced connectivity extend direct command and control from the front lines to operational or strategic level headquarters. Therefore, the command and control structure for Generation Z needs to be modified in a way that, regardless of the future technical developments the Armed Forces embrace, will allow tactical commanders to maintain enough flexibility and scope for initiative. The employment of contemporary technology would raise the issue of

whether the military should reduce manpower by replacing many of its duties with computers and machines. However, given the population versus employment scenario, new ideas must be developed to utilize this extra labor in other important responsibilities rather than removing them from the services. More digitalization would increase the security risks to military data and the cyber network. A joint cyber command may be formed to combat cyber threats, with the nation's civilian cyber experts effectively incorporated. In conclusion, Generation Z commanders would value the advantages of contemporary technical advancement in their command and control systems, notwithstanding a few challenges that can be overcome by making wise and calculated decisions.

References

1. Abu Ashraful Haider, 'What will Bangladesh look like in 2050?', The Daily Star, 14 April 2018.

2. 'Bangladesh: Internet users', The Global Economy, 2020, available at: www.theglobaleconomy.com/ Bangladesh/Internet_users/. Accessed on 01 May 2023.

3. 'Bangladesh now 35th largest economy in the world', The Dhaka Tribune, 06 January 2023, available at: https://www.dhakatribune.com/bangladesh/2023/01/06/bangladesh-now-35th-largest-economy-in-the-world. Accessed on 01 May 2023.

4. Daphne Leprince-Ringuet, "Fewer troops, but more tech: Military downsizes as it shifts to AI, drones and cyber", Innovation, 23 March 2021.

5. 'Every village to be connected by fibre optical cable by 2025: Palak', The Business Standard, 31 January 2022, available at: https://www.tbsnews.net/bangladesh/every-village-be-brought-under-fibre-optic-cable-2025-palak-364636. Accessed on 02 May 2023.

6. John Twenge, 'How are generations named?', Trend, Winter 2018 issue, 26 January 2018.

7. Lieutenant Colonel Rosario M. Simonetti, 'Automation and the Future of Command and Control:

8. The End of Auftragstaktik?', Marine Corps University Journal, Volume 11, No 1, 01 November 2020.

9. 'National Strategy for Robotics', Information and Communication Technology Division, Government of the People's Republic of Bangladesh, September 2020.

10. 'National Strategy for Artificial Intelligence', Information and Communication Technology Division, Government of the People's Republic of Bangladesh, March 2020.

11. 'National Internet of Things Strategy Bangladesh', Information and Communication Technology Division, Government of the People's Republic of Bangladesh, March 2020.

12. Simon Kemp, 'Digital 2024: Bangladesh', Data Reportal, 23 February 2024, available at: https://datareportal.com/reports/digital-2024-bangladesh. Accessed on 02 May 2024.

13. Steve Boatright, Lt Col. 'The Millennial Generation and the Military'. Air War College. 11 February 2016.

14. Wachowiak, Cassandra M. 'Generational Diversity in Military Leadership: Exploring Challenges and Opportunities'. University of New Hampshire College of Professional Studies. 29 April 2024.

Author

Colonel S M Moniruzzaman, SGP, afwc, psc was commissioned in 1998 with 38th BMA Long Course. During his military career, the officer not only served in several signal regiments but also held the positions of Brigade Major in a signal brigade, Second-in-command in a signal battalion, and commanded a signal battalion in an operational division. In addition, he served as an instructor at the schools of both Signals and Military Intelligence and as the General Staff Officer-1 (Operations and Training) in Headquarters Army Training and Doctrine Command. He graduated from Defence Services Command and Staff College and National Defence College, Mirpur. The officer was awarded Sena Gourab Podok for his outstanding contribution to Operation Twilight in 2017. He is currently the Principal of Shaheed Bir Uttam Lt. Anwar Girls' College, Dhaka Cantonment.

NDC JOURNAL
Security Through Knowledge

ECO-TOURISM AS A CATALYST FOR SUSTAINABLE DEVELOPMENT IN THE SOUTH-WEST REGION OF BANGLADESH

Lieutenant Colonel G M Mamunur Rashid, psc, G+, Air Defence

Introduction

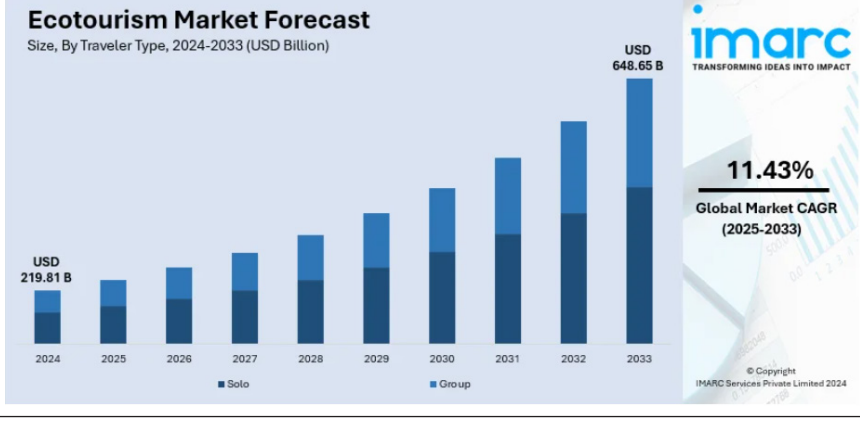
Eco-tourism is a way of sustainable tourism based on the unique features; such as culture, natural beauty, biodiversity etc. of any particular area. It also relates to generating economic benefits, ensuring societal welfare for the locals and conserving the environment of that place. Eco-tourism has the potential to bring sustainable development in developing countries like Bangladesh. In this paper, 16 districts of Khulna and Barisal divisions, and a few neighboring districts (districts located on the south-west side of Padma and Meghna river) are considered as south-west region. These areas are enriched with biodiversity, unique culture, beautiful landscapes and so on. Despite of having much potentials, this region is struggling to implement eco-tourism and leverage sustainable development due to several issues such as inadequate infrastructure, socio-economic drawbacks, lack of research, comprehensive data and many other issues.

In 2024, the global market for ecotourism is estimated at US$ 219.81 It is expected to reach US$ 648.65 billion by 2033, demonstrating an 11.43% (Figure 1) rise in the ecotourism market from 2025 to 2033 (IMARCGROUP, 2024). According to a report from 2022 by the Bangladesh Bureau of Statistics, it is evident that tourism contributes to 3.02% of the GDP which amounts to Tk 76,690.7 crore. Again, more than 8% of the total employment of the country comes from this sector (Byron and Hasan, 2021). According to the Travel and Tourism Development Index 2024, Bangladesh is ranked 109th among 119 countries internationally (Figure 2), scoring the lowest in sustainability (The Business Standard, 2024d). Implementing ecotourism in the south-west region can boost local

sustainable development and help Bangladesh to improve its ranking in the travel and tourism index. Consequently, eco-tourism leads to the development of societal facilities and infrastructures in the surrounding areas which is evident in the case of the Sundarbans. Hence, it would be beneficial for the south-west region as well.

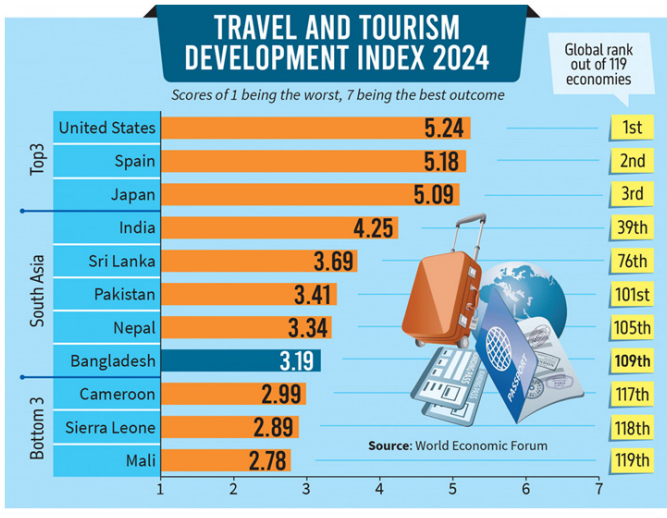
Considering this significance, eco-tourism can be prioritised as a key strategy to ensure sustainable development in the south-west region of Bangladesh. In today's world, tourism plays a very vital role in economic growth and sustainable development for many countries. Notable examples around Bangladesh are Maldives, Thailand, Nepal, and Singapore. At this backdrop, the primary objective of this study is to explore how eco-tourism can serve as a catalyst for sustainable development in the south-western region of Bangladesh by identifying its potential benefits and challenges.

Figure 1: Ecotourism Market Size Forecast



Source: IMARCGROUP, 2024

Figure 2: Bangladesh's Ranking in Travel and Tourism Development Index 2024



Source: The Business Standard, 2024

Literature Review

Polash and Habeb (2020) highlighted that eco-tourism can be used as a way of ensuring sustainable development by leveraging the societal, economic, and environmental benefits it offer. In the context of south-west region of Bangladesh, this broader framework of sustainable development can significantly accelerate the process and progress in advancing society, economy, and environment in the long term. According to Afroz and Mahmud (2017) ecotourism can contribute to sustainable development by addressing the present problems while remaining viable for future issues. This approach is also applicable to the south-west region. Hence, it is important to study eco-tourism and its impact on sustainable development in the south-west region to understand and devise a proper eco-tourism policy.

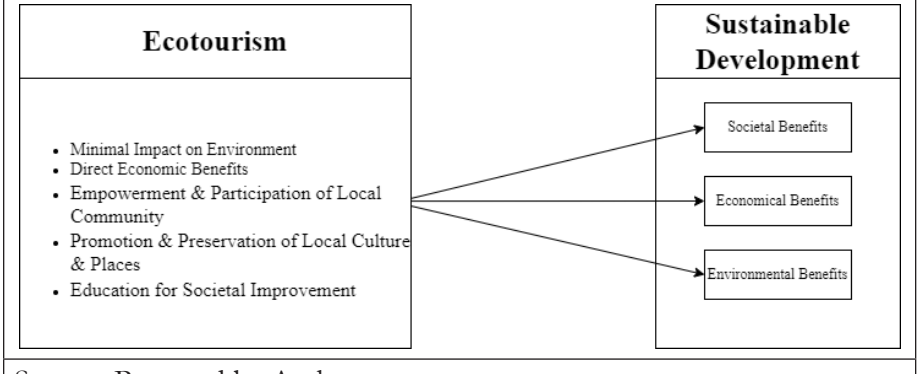
In Bangladesh, many researches have been conducted on eco-tourism and sustainable development separately and also their focus remained on the south-east region like Chattagram and Sylhet. There is a lack of research on

the south-west region. Besides, previous studies often showed the impact of eco-tourism without connecting to sustainable development. Hence, this study aims to fill these gaps by exploring how eco-tourism can help as a transformative tool for sustainable development in the south-west region of Bangladesh.

Methodology

This research utilized an inductive research strategy as it aims to explore the patterns and theories from collected data rather than testing hypothesis. Additionally, as this research is the first of its kind in the south-west region, the primary research approach has been adopted by the author in order to collect fresh, context-specific data. The population size of this research incorporates various types of stakeholders such as local people, eco-tourism operators, government officials, and tourists. In terms of sampling, the author employed a purposive sampling technique. This study utilised both quantitative and qualitative data. To collect quantitative data, a survey method has been utilised with semi-structured questions, while qualitative data has been collected through interviews with local residents and a review of previous reports and articles. This study applied both statistical analysis and content analysis to quantitative data and qualitative data respectively.

Figure 3: Conceptual Framwork

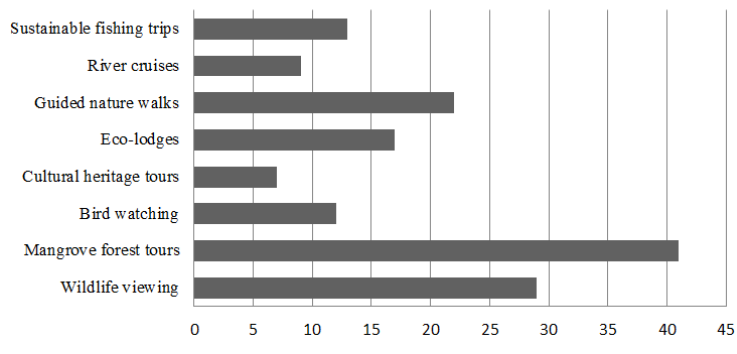


Source: Preapred by Author

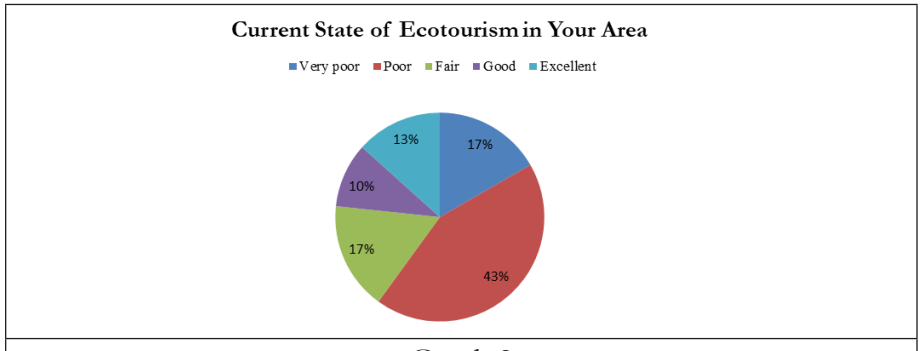
Findings and Discussion

Current State of Eco-tourism in the South-West Region

The south-west region of Bangladesh always had the potential for eco-tourism due to its enriched culture, natural landscape, diverse wildlife, historical monuments, and unique heritages (Hossain and Haider, 2016). Sundarbans and Kuakata are two well-recognised sites among the existing natural eco-tourism sites in the region. Bangladesh Economic Zones Authority (BEZA) is planning to establish an ecotourism park in Bagerhat (Mirdha, 2022). In the south-west region, the main eco-tourism activities include exploring Mangrove Forests, Wildlife Sanctuary, and Nature walking with guides. Respondents agreed that, there are other areas, such as different Mosques and Mandirs in Bagerhat and Satkhira, Bird watching in Faridpur, Fishery projects in Khulna, Jamider Bari and Eco-lodges in Satkhira, Cultural heritage tours in Khustia, and Sustainable fishing trips in Bagerhat which are not been explored to the optimum (Graph 1). Ashekuzzaman, a local resident from Jhenaidah, shares, "There are many potential sites in my area that could be utilized as ecotourism spots but have not been highlighted that much." Due to this lack of promotion, the south-west region's eco-tourism remained comparatively underdeveloped.



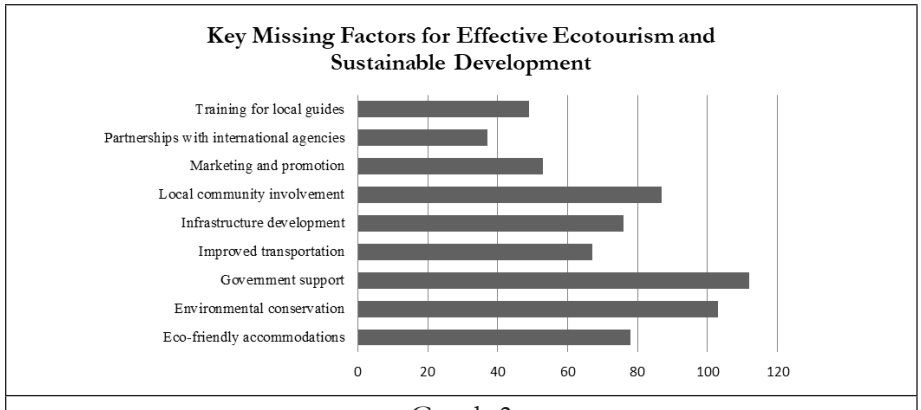
Graph 1



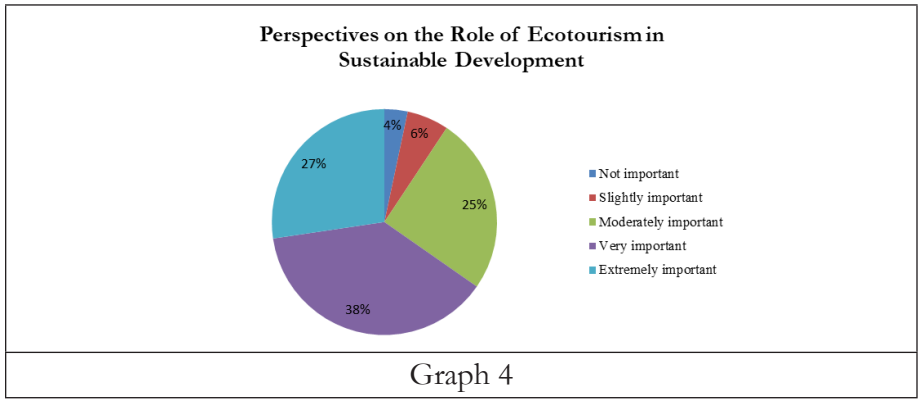
Graph 2

Apart from the recognised sites in the region, there are more than 100 sites such as Chanchra Palace, Rakhal-Shah Shrine, Kaludanga Temple, One-Domed Mosque, Jahajghata Naval-Fort, Flower-Village Godkhali, Laldia Beach, Char Kukri-Mukri, Haringhata Reserved-Forest, Sonarchar Wildlife-Sanctuary, Pink Village, Aamjhupi Neel-Kuthi, Shapla Village, and Sreepur Jomidar-Bari etc with potential for eco-tourism that remained unrecognized and under-promoted. Lack of development works and inadequate promotion, which has hampered their ability to provide ecotourism and sustainable development benefits (Tourist Places, 2023). Integrating these sites into a comprehensive ecotourism policy can bring considerable improvements in other sectors such as economy, environment, infrastructural development etc. which in turn can lead to sustainable development in the region. This situation is evident from responses of survey participants (Graph 2). Over 55% of the participants agreed that the condition of eco-tourism is poor and many areas are under-valued in their areas due to various barriers and challenges. In the south-west side of Bangladesh, eco-tourism activities are very narrow and less structured. Already well-known tourist places are suffering from negligence, lack of policy and preservation. Illegal logging, littering, and poaching are happening on a daily basis, presenting various significant threats to eco-tourism in the region. Moreover, the lack of co-management structure between government and local stakeholders is one of the major reasons behind this under-development of eco-tourism which is hindering

sustainable development. Survey participants also agreed that there are some important missing factors in the south-west region that could have supported eco-tourism (Graph 3). Only traditional supporting factors are available, which are not adequate. As a result, the overall progress is very slow.



Graph 3



Graph 4

Respondents also believe that eco-tourism can play an important role in terms of ensuring sustainable development in the south-west region (Graph 4). For example, many infrastructures have been developed, employment increased in the area around the Sundarbans. Now, if the same kind of attention is given to other areas, then the positive impact of eco-tourism would ensure sustainable development in the south-west region.

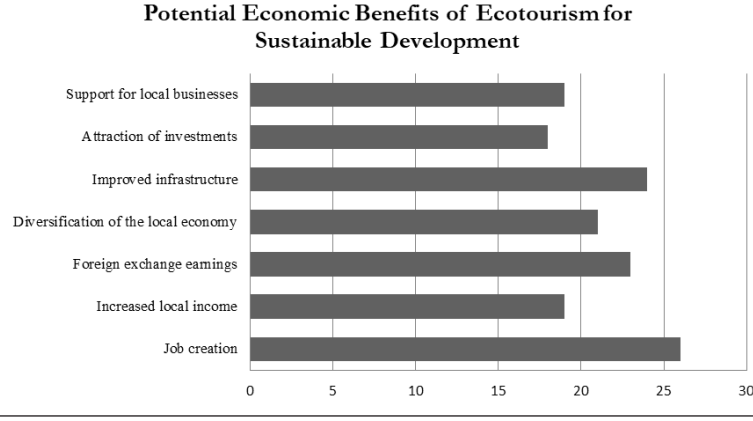
Overall, the current state of eco-tourism in the south-west region is underdeveloped but shows promises. With effective investment and efforts, impending benefits of eco-tourism can be obtained and utilized as a tool for ensuring sustainable development.

Impending Benefits of Eco-tourism in the South-West Region

The benefits of eco-tourism can be categorised into three aspects: economic, societal and environmental. The following sections explain how these benefits can lead to sustainable development in the region.

Economic Benefits

Eco-tourism has the potential to boost the economy of the south-west region significantly. It can help to create new job opportunities, generate revenue and strengthen the local economy, as stated by the survey respondents (Graph 5). Some of these economic benefits are discussed below:



Graph 5

- **Creation of New Jobs and Increased Local Income.** Developing eco-tourism can create new job opportunities in the category of

managers, staff, cooks, transporters, and tour guides, and boost income for local people (Majumder, 2020). For instance, at Sundarbans, local Harbaria villagers carry passengers, sell food, and work at the Harbaria Eco-tourism Centre and thus earn their livelihood. Similarly, a local resident from Chuadanga shares, "Many local youths are involved in businesses targeting eco-tourism spots here. Two of my friends and I also work at DC Park in Damurhuda as cleaner and night guards, I sell fast-food during day and do duty at night. This eco-tourism park has provided us with employment and opportunity to earn extra income". Eco-tourism has led to a 30% increase in job creation while boosting household income by 50% (The Financial Express, 2024b). These exemplifies how eco-tourism can generate employment for the locals, resulting enhanced income sources.

- **Foreign Exchange Earnings and Attraction of Investments.** Eco-tourism can bring foreign currency and investments to the South-west region. Various local sources suggest that foreign visitors stop at different sites like Chandpai Range in Khulna, Dublar Char in Satkhira when visiting the Sundarbans. It brings foreign currency. Similarly, a local young entrepreneur of Satkhira's Kaliganj informed that he had already started experiencing small-scale reservations by foreign tourists. He also stated that he had been approached with proposals to invest in his eco-cottage by some inividual. Exploring further, it was revealed that many ogrnisations and inividuals are investing in these areas to explore this opportunity. For example, new hotels, restaurants, transportation, conference halls, and institutes are being built in the south-west region around tourist sites.

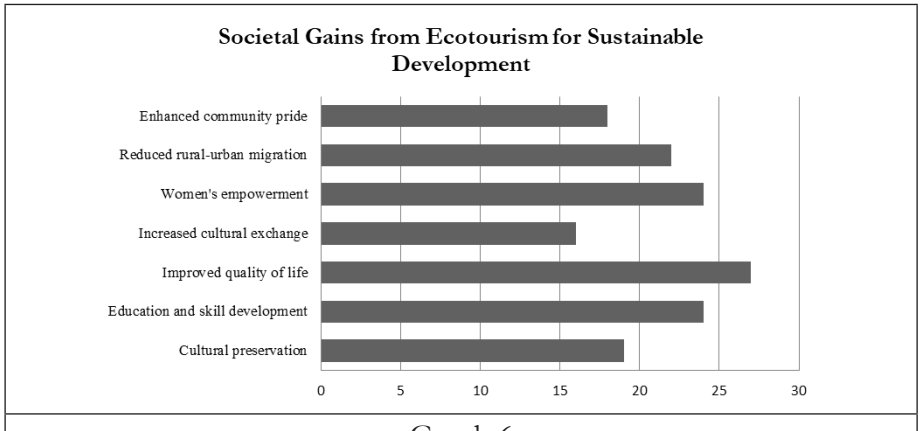
- **Diversification of the Local Economy and Support for Local Businesses.** Eco-tourism can help to reduce dependence on agro-industry, diversify the local economy, and create support for local businesses in the South-west region. Traditionally reliant on agriculture and fishing, this region is experiencing a progressive change. Over 500,000 tourists explore the surrounding places while visiting the

Sundarbans, contributing roughly US$ 50 million to the local economy annually (The Financial Express, 2024b). Eco-tourism opened the door of new economic activities such as selling local handicrafts, souvenirs, accommodation and foods, readymade clothes etc (Siddiqua, 2022). In this way, eco-tourism can diversify the local economy while strengthening local businesses in the south-west region.

Besides the discussed points, eco-tourism has other economic benefits. For example, it can boost local craftsmanship, support regional branding, improve property value, bring foreign investment, and increase tax revenues.

Societal Welfares

Various societal welfare is related which come as a complimentary benefit from Eco-tourism (Graph 6). These benefits can strengthen the local community further by ensuring sustainable development in the society.



Graph 6

- **Preservation of Local Culture and Heritage.** Eco-tourism has the potential to preserve local culture, heritage and enhance the life of different religious communities in the south-west region. Eco-tourism helps to showcase, promote and celebrate the local arts, culture, and practices. For example, local festivals like the Ras Mela at Dubla, the

Lalon Mela and Dol Purnima in Kushtia, and the Gurpukur Mela in Satkhira are fading day by day, which were more vibrant in the past (Khokon, 2021). Promoting these local cultures under eco-tourism can attract both foreign and local tourists to visit and experience these unique heritages and cultures. In this way, eco-tourism helps to preserve local culture, heritage, and community by making them feel included and valued within the social domain.

- **Education, Skill Development and Improved Quality of Life.** Eco-tourism has the capacity to lead to substantial improvements in education and skill development in the south-west region. Eco-tourism stimulates demand for educated population, skilled man-power and sustainable actions, hence driving investments in training programs and educational initiatives to meet these needs. Sustainable tourism associated organisations like Environment and Social Development Organization (ESDO) is working with local residents in the region to improve quality of life through healthcare, education, training, and income-generating activities (ESDO, 2024).

- **Less Urban Migration and Women Empowerment.** Eco-tourism can also help to ensure gender equality and women empowerment in the south-west region. It creates opportunities for all genders. As a result, many educated women have the opportunity to work in eco-parks and engage in businesses associated with eco-tourism. Correspondingly, eco-tourism can also solve the problem of urban migration by creating better prospects and facilities like Dhaka, encouraging local people to stay in their locality. Mrs Rahima, a local housewife and owner of a small business in Bagerhat, mentioned that she had a traditional sweets business in her village as it is popular among tourists. Earlier, she used to work in Dhaka as a house-maid.

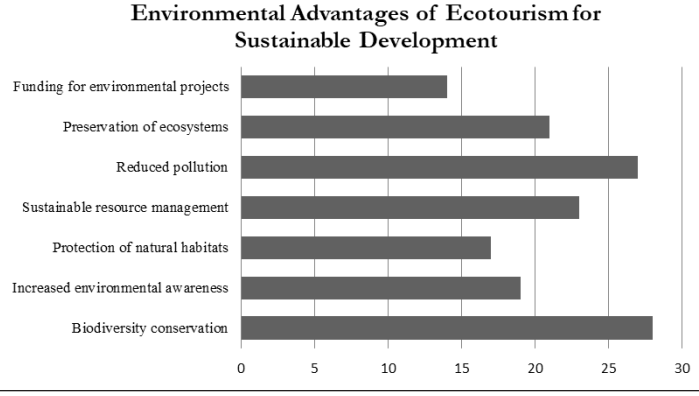
- **Development and Improved Infrastructure.** Eco-tourism can also drive infrastructural development in the south-west region, benefiting both tourists and residents. For example, Gollamari Bridge on the Mayur River and Kalna Bridge on Gopalganj's Madhumati River are

being constructed, enhancing connectivity to key eco-projects and improving infrastructure in the south-west region (The Daily Sun, 2020). Another example would be, the natural attraction of Talsari Road in Chuadanga's Shiv Nagar has led to the development of infrastructures, such as roads, small hotels and shops, clean water, sanitation, and hospitals in the area. This shows that development and eco-tourism are complimentery to each other.

Apart from these major benefits, eco-tourism also helps in other areas such as local innovation, the health sector, community pride, cultural exchanges and largely social resilience in the region.

Environmental Advantages

Eco-tourism mechanism helps to preserve environmental resources and ecosystems (Graph 7). These environmental benefits help to protect wildlife and natural habitats which are the main attractions of the south-west region.



Graph 7

- **Biodiversity Conservation and Habitat Protection.** Eco-tourism can help to preserve natural habitats and biodiversity in the south-west region. Research suggests that eco-tourism activities have led to a 40% boost in the population of local endangered species and a 25% decline

in poaching (The Financial Express, 2024b). Dr H.M. Irfanullah, an environment and climate change consultant, stated that biodiversity conservation can be ensured through tourism (The Daily Star, 2024). This benefit aligns with and can be achieved through eco-tourism principles. Similarly, local residents are learning about the benefits of eco-tourism and it is encouraging them to take care of natural resources, reducing illegal hunting and deforestation. Furthermore, various biodiversity-related laws have been formulated to protect eco-tourism spots, such as Ecologically Critical Area Management 2016 and Bangladesh Biodiversity Act 2017, illustrating eco-tourism's positive impact. Overall, these efforts demonstrate how eco-tourism can support environmental conservation and community engagement.

- **Increased Environmental Awareness and Sustainable Resource Management.** Eco-tourism is a type of responsible tourism. Environmental awareness among under-developed areas and local communities can be increased through it. Various informative tours and programs in Jessore, Bagerhat, and Khulna have already been arranged to inform visitors about the exceptional environmental aspects of the south-west region. Furthermore, eco-tourism also promotes sustainable resource management. For example, NGO like Local Environment Development and Agricultural Research Society (LEDARS) works with local people to raise awareness of utilising resources in a sustainable manner (LEDARS, 2019). In this regard, local communities and businesses are motivated to adopt nature-friendly practices, and use green energy, not over-exploiting natural resources such as fish, food, or animals.

- **Preservation of Ecosystems and Reduced Pollution.** Geographically the South-west region is vulnerable to natural disasters such as cyclones, floods etc. Eco-tourism can be used as a tool to ensure the protection of ecosystems from natural risks. At the same time, effective eco-tourism can also lead to reduced pollution, utilisation of green energy, and waste management in the region. Supporting this vision, Honourable

Chief Adviser to the interim government, Professor Dr. Muhammad Yunus, has already offered a proposal to Chinese Ambassador Yao Wen to relocate some Chinese solar panel manufacturing plants to Bangladesh (The Financial Express, 2024). This reflects the current interim government's commitment to the country's green transition and, consequently, aligns with eco-tourism principles supporting sustainable development. Similarly, eco-conscious travellers also prefer eco-tourism sites where waste management, recycling facilities and conservation practices are ensured. Use of Solar panels, reduction of plastic packaging and bottles, and utilising recyclable goods are already in progress in some areas like Rajbari, Shatkhira, Khulna and other districts.

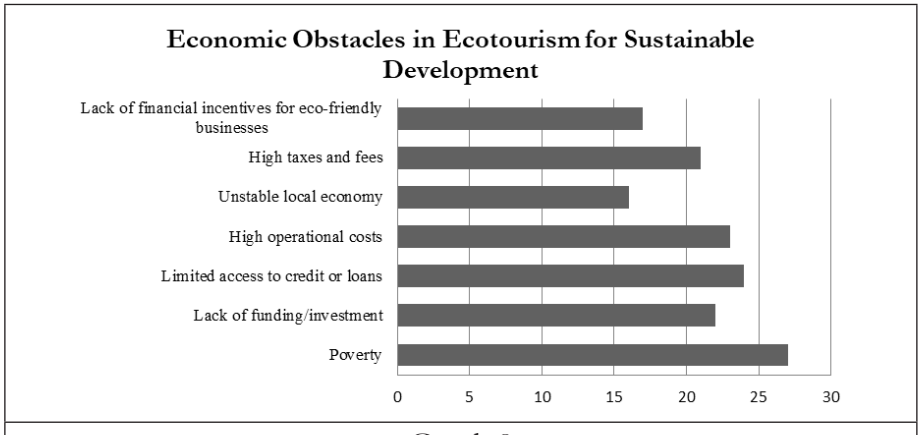
Beyond these key benefits, eco-tourism also helps in areas like climate change mitigation, ecosystem resilience, and preservation of locally unique landscapes and species, ensuring sustainable development in the south-west region.

Imminent and Existing Barriers of Eco-tourism in the South-West Region

Implementing eco-tourism in the south-west region is a difficult task due to the lack of proper foundation and support for eco-tourism. The current conditions in the south-west region possess several imminent and existing barriers. These obstacles need to be addressed properly to utilise eco-tourism as a development tool in the region.

Economic Constraints

Economic hurdles can hamper the implementation of eco-tourism in the south-west region significantly, as highlighted by respondents (Graph 8). The major economic constraints are:



Graph 8

- **Poverty.** Poverty is a critical and common constrain for eco-tourism in the South-west region of Bangladesh. Many areas of the south-west side of Bangladesh are suffering from poverty problems. This situation is limiting the mindset of the local communities and hampering the investment in infrastructure and societal services, but ecotourism has the potential to alleviate poverty as well. Many interested local residents cannot start eco-tourism-related small and medium businesses, hence, it would make eco-tourism difficult to implement.

- **Lack of Funding, Investment and Credit.** Eco-tourism is a sensitive project where funding and loans are invested in a calculated way. However, there is a lack of investment from both public and private organisations due to various problems. This lack of money may restrict eco-tourism activities in the region and sustainable development. Again, inadequate funding in eco-tourism limits the potential benefits of eco-tourism, which could negatively impact local entrepreneurs in the region. This issue may create problems for interested parties to implement eco-tourism in the region.

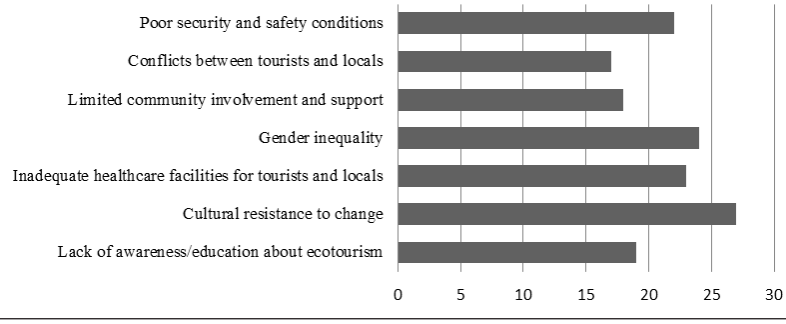
- **High Operational Costs and Lack of Certification.** Developing eco-tourism is challenging due to heavy operational costs and the need for certification. Again, high taxes and fees are creating a heavy

burden on the shoulders of local entrepreneurs. The current taxation policy, includes 15% on services, 5% on purchased goods, and 5% on revenue, totalling a 25% percent value added tax (VAT), in the south-west region is not suitable for big eco-tourism projects (The Daily Star, 2022). Mr Shajal, a small business owner in Satkhira, says, "The costs of everything are increasing continuously, and it has become difficult for me to keep my business running." In line with this, Md Rafeuzzaman, President of the TOAB, argues the entire tourism sector is suffering from inappropriate taxation policy and urges to remove 15% tax in the Fiscal-Year (FY) 2025 (The Business Standard, 2024c). Thus, these high taxes and VAT are contributing to the high operational costs and impeding the development of the eco-tourism businesses in the region.

Beyond these economic constraints, some other major economic issues noted by respondents are unstable local economy, lack of business-friendly environment, inadequate support from financial institutions etc.

Societal Issues

Societal obstacles can delay eco-tourism development and hinder sustainable development in the south-west region (Graph 9). Some of the key societal challenges are discussed below.



Graph 9

- **Resistance to Change and Lack of Community Involvement.** Resistance by local people to the changes brought by eco-tourism can make it ineffective. The most significant issue that would arise from eco-tourism in the south-west region would be cultural resistance to the new change. Mamun Molla, a resident from Gopalganj informed that 'the local people sometimes don't like the heavy flow of tourists as it is disturbing their daily lives and traditions. They feared that their culture and women would get spoiled by these exposures'. The old-styled norms, mindsets, and customs in the region sometimes clash with the modern trends of tourism. As a result, promoting eco-tourism in some of the areas would become difficult. This brings a new thought that eco-tourism practices must be culturally sensitive in some of the areas.

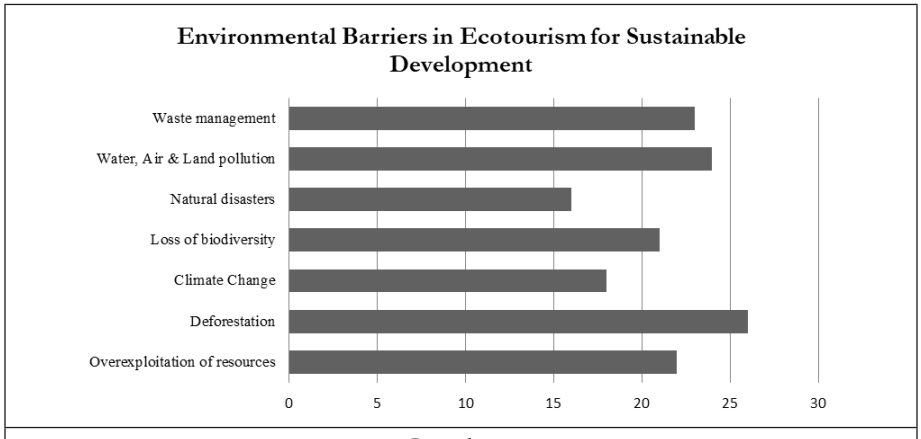
- **Inadequate Infrastructures and Gender Inequality.** Without social facilities and infrastructures such as healthcare, education for both boys and girls, etc, eco-tourism cannot be explored properly. Again, due to the lack of roads, stores, safety, and societal infrastructures, many entreprenuers don't want to invest in eco-tourism business (Hasan, 2022). But the matter of hope is that these situations are changing gradually. As a result, both tourists and local communities may suffer and sustainable development would not work.

- **Poor Security and Safety Conditions.** Lack of proper security and safety in the south-west region poses a big threat to eco-tourism and hinders overall sustainable development. Political instability, natural disasters, and high crime rates are high in some districts like Jhenaidah, Bagerhat, and Jessore. Golam Rasul, a local resident from Shailakupa of Jhenaidah mentioned that, almost every day, political and societal conflict occurs in his area which would hinder the efforts to promote and develop eco-tourism. Similarly, sometimes businessman has to pay bribe to local political leaders and gangs which is also hampering eco-tourism activities (The Business Standard, 2024a). This shows how lack of security and safety can derail eco-tourism efforts and sustainable development in the region.

Besides, some other significant challenges such as lack of awareness, inadequate training and skill development, and insufficient government investment need to be addressed as well.

Environmental Challenges

Environmental challenges create a major obstacle against the development of eco-tourism and ensure sustainable development in the south-west region (Graph 10). Some of the major environmental challenges are illustrated below:



Graph 10

- **Deforestation and Loss of Biodiversity.** One of the major environmental challenges for eco-tourism is the deforestation and loss of biodiversity. The development of eco-tourism-related or supporting infrastructures sometimes leads to loss of biodiversity and deforestation. For example, Bridges, road construction and other supporting mega development projects like Rampal Power Plant in the southwest region are having negative impact on environment and biodiversity (Hossain, 2022). Hence, ineffective establishment of eco-tourism spots can lead to deforestation, disruption of wildlife, and degradation of natural habitats. Furthermore, this aggressive rate of developing eco-tourism spots can reduce nature's resilience to stand against climate change and natural disasters.

- **Air, Water and Land Pollution.** A core challenge that can hamper eco-tourism and sustainable development is air, water, and land pollution. For example, wastage discharged by tourists lead to land and water pollution in coastal area in Kuakata and mangrove forests in Sundarbans. Addresing this problem, Environment, Forest, and Climate Change Adviser to the interim government of Bangladesh, Syeda Rizwana Hasan has announced an urgent action to clear these areas of plastics and other waste, highlighting the pollution issue (The Business Standard, 2024b). This pollution is not only hampering human life, but also hampering the aquatic and wildlife.

- **Overexploitation of Resources.** One of the subtle but definite challenges that comes from eco-tourism is the excessive exploitation of resources. Eco-tourism would open the door for many leisure activities but often these activities cross limits such as poaching, overfishing, destroying forests, illegal logging, and forceful unsuitable agronomic practices. In this regard, Advisor Syeda Rizwana Hasan emphasized the need for an Integrated Plan and 'Zero Waste Action Plan' to ensure sustainable development by developing ecotourism, especially in Payra Port City and the Kuakata coastal region (BSS News, 2024).

Apart from these major challenges, some other issues which need to be addressed are waste management, soil degradation, climate change, and extreme urbanisation.

Recommendations

Eco-tourism brings a wide range of benefits which in turn would compliment to sustainable development in the south-west region of Bangladesh. To exploit these benefits and mitigate barriers, few effective steps need to be taken by government and private organisations. Basing on the above discussion, some recommendations are apended below:

- An effective and comprehensive policy regarding eco-tourism for the south-west region should be developed immediately. The policy must incorporate action plans, strategies regarding eco-tourism activities and principles fulfilling international standards.
- Development of various social and eco-friendly organisations should be funded and developed, such as hospitals, hotels, SMEs, educational institutions etc. The use of renewable energy and management of waste should be prioritised. Standard eco-friendly practices should be incorporated into these infrastructures.
- Marketing and branding tactics should be devised by government and private organisations collaboratively for international and local tourists. The unique culture, nature, and history of the south-west region should be promoted through visual media to attract tourists globally.
- Local people should be trained in terms of eco-tourism, hospitality and other tourism related skills so that eco-tourism can be implemented and run effectively. Local involvement is also important and needs to be ensured so that a mindset of eco-tourism and sustainable development can grow among the locals.
- Partnerships with international tourism and development organisations need to be developed. By partnering with these organisations in the eco-tourism business, the south-west region can benefit from funding, expertise and global promotion.
- Lastly, a strong and independent south-west regional eco-tourism authority may be established. A proper collaboration among stakeholders needs to be managed and continuous assessment of the environmental, economic, and social impacts of eco-tourism needs to be conducted. The assessment report would help to rearrange and improve strategies for sustainable development in the area.

Conclusion

Bangladesh, particularly the south-west region, has all kinds of potential resources to ensure sustainable development and eco-tourism can serve as a transformative force to trigger and ensure this transformation. The south-west region of Bangladesh has remained comparatively less developed part of the country for many years. This region is perfectly suited for eco-tourism with its natural beauty, unique culture, enriched history, heritage, and diverse wildlife. However, eco-tourism conditions in this area have remained underdeveloped for the lack of proper attention and guidance. Eco-tourism offers several opportunities and benefits for this region such as economic growth, social welfare, and environmental conservation. However, there are several obstacles as well, such as inadequate infrastructure, natural disaster, and financial constraints. Addressing these obstacles and leveraging the benefits would be the main challenge for the relevant parties. Several key steps can be taken such as comprehensive policies, community involvement, international partnership, and research and monitoring to overcome these issues. Government, private organisations, and NGOs should come together to work on eco-tourism projects to ensure that local communities receive proper benefits. In conclusion, it can be said that effective and efficient implementation of eco-tourism can be used as a powerful catalyst for ensuring long-term sustainable development in the south-west region.

References

1. Afroz, N. and Mahmud, Md.S. (2017). Analyzing The Problem And Prospects Of Ecotourism: A Review On Bangladesh. IOSR Journal of Business and Management, 19(05), pp.59–65. doi:https://doi.org/10.9790/487x-1905035965.
2. BSS News (2024). Integrated plan a must for developing ecotourism, protecting coastal areas: Rizwana. Bangladesh Sangbad Sangstha. [online] 28 Nov. Available at: https://www.bssnews.net/news-flash/226949 [Accessed 29 Nov. 2024].

3. Byron, R.K. and Hasan, M. (2021). Tourism's share 3.02% in GDP. [online] The Daily Star. Available at: https://www.thedailystar.net/business/economy/industries/tourism/news/tourisms-share-302pc-gdp-2904556 [Accessed 24 Aug. 2024].

4. ESDO (2024). Community based Eco-tourism - ESDO. [online] ESDO - Environment and Social Development Organization. Available at: https://esdo.org/community-based-eco-tourism/ [Accessed 5 Sep. 2024].

5. Hasan, R. (2022). Red tape, poor infrastructure, holding back tourism in Bangladesh. The Daily Star. [online] 27 Sep. Available at: https://www.thedailystar.net/news/bangladesh/news/tourism-bangladesh-poor-infrastructure-red-tape-holding-it-back [Accessed 10 August 2024].

6. Hossain , M.H.H. (2022). Rampal power plant: Experts stress strict monitoring during operation. Dhaka Tribune. [online] Available at: https://www.dhakatribune.com/bangladesh/293599/rampal-power-plant-experts-stress-strict [Accessed 2 August 2024].

7. Hossain, T. and Haider, M.Z. (2016). Sustainable Tourism Development in the South-West Region of Bangladesh . Journal of Investment and Management, 5(6), pp.193–198. doi:https://doi.org/10.11648/j.jim.20160506.24.

8. Hossen, M.B. (2022). Eco-tourism shows the way. [online] Dhaka Tribune. Available at: https://www.dhakatribune.com/opinion/op-ed/296894/eco-tourism-shows-the-way [Accessed 24 Aug. 2024].

9. IMARCGROUP (2024). Ecotourism Market Size, Trends | Global Industry Report 2021-2026. [online] www.imarcgroup.com. Available at: https://www.imarcgroup.com/ecotourism-market [Accessed 20 Oct. 2024].

10. Khokon, L.H. (2021). হারিয়ে যাওয়া মেলা. Jugantor. [online] Available at: https://www.jugantor.com/todays-paper/editorial/387340 [Accessed 5 Sep. 2024].

11. LEDARS (2019). About us - Local Environment Development and Agricultural Research Society. [online] Local Environment

Development and Agricultural Research Society. Available at: https://www.ledars.org/aboutus/ [Accessed 2 Sep. 2024].

12. Majumder, Dr.A.K. (2020). Eco-tourism: An Opportunity for Bangladesh. The Daily Sun. [online] Sep. Available at: https://www.daily-sun.com/printversion/details/508803/Ecotourism:-An-Opportunity-for-Bangladesh [Accessed 9 Sep. 2024].

13. Mirdha, R.U. (2022). 17 economic zones getting ready for south-west. The Daily Star. [online] 29 Jun. Available at: https://www.thedailystar.net/business/economy/news/17-economic-zones-getting-ready-south-west-3059196 [Accessed 22 Aug. 2024].

14. Polash, A.K. and Habeb, A. (2020). Ecotourism: A new door to possibilities for Bangladesh . International Journal of Advances in Engineering and Management (IJAEM), 2(8), pp.121–132.

15. Siddiqua, T. (2022). Ecotourism: New Approach To Economic Development In Bangladesh. Khulna University Studies, pp.137–144. doi:https://doi.org/10.53808/kus.2006.7.1.0548-s.

16. The Business Standard (2024a). Bribery, corruption main obstacles in promoting business in Bangladesh: US report. The Business Standard. [online] 31 Mar. Available at: https://www.tbsnews.net/economy/bribery-corruption-main-obstacles-promoting-business-bangladesh-us-report-819351 [Accessed 10 June 2024].

17. The Business Standard (2024b). St Martin's, Kuakata, Sundarbans to be made plastic-free: Rizwana. The Business Standard. [online] Available at: https://www.tbsnews.net/bangladesh/environment/st-martin-kuakata-and-sundarbans-be-made-plastic-free-rizwana-927276 [Accessed 28 August 2024].

18. The Business Standard (2024c). Toab demands withdrawal of 15% VAT on tourism sector. The Business Standard. [online] 8 Jun. Available at: https://www.tbsnews.net/economy/budget/toab-demands-withdrawal-15-vat-tourism-sector-871881 [Accessed 10 June 2024].

19. The Business Standard (2024d). Travel and Tourism Development Index 2024: Bangladesh ranks last in Asia-Pacific. The Business Standard. [online] 21 May. Available at: https://www.tbsnews.net/bangladesh/travel-and-tourism-development-index-2024-bangladesh-ranks-last-asia-pacific-857201 [Accessed 21 Aug. 2024].

20. The Daily Star (2022). Current VAT, tax rates big obstacle in tourism sector development: JS body. The Daily Star. [online] 24 Aug. Available at: https://www.thedailystar.net/life-living/travel/news/current-vat-tax-rates-big-obstacle-tourism-sector-development-js-body-3102321 [Accessed 24 August 2024].

21. The Daily Star (2024). Bangladesh's way forward to biodiversity conservation. [online] The Daily Star. Available at: https://www.thedailystar.net/opinion/views/news/bangladeshs-way-forward-biodiversity-conservation-3651096 [Accessed 24 Aug. 2024].

22. The Daily Sun (2020). Kalna Bridge to ensure faster communication in south-western region. [online] daily-sun. Available at: https://www.daily-sun.com/printversion/details/471621 [Accessed 24 Aug. 2024].

23. The Financial Express (2024). Prof Yunus urges China to relocate solar panel plants to Bangladesh. The Financial Express. [online] Available at: https://thefinancialexpress.com.bd/home/china-urged-to-relocate-solar-panel-plants-to-bangladesh [Accessed 26 August 2024].

24. The Financial Express (31 Mar 2024). Green Entrepreneurship: Scope for youth employment in Bangladesh. Available at: https://thefinancialexpress.com.bd/green-entrepreneurship-scope-for-youth-employment-in-bangladesh [Accessed 12 Jun 2024].

25. Tourist Places (2023). Find Nature Attractions and Other Attractions to Visit in Bangladesh. [online] www.touristplaces.com.bd. [Accessed 5 August 2024].

Author

Lieutenant Colonel G M Mamunur Rashid, psc, G+ was commissioned on 27 December 2001 with 45th BMA Long Course. In his military profession, he has served in five Units, including commanding an Air Defence Regiment. His other mentionable service experience includes General Staff Officer, Grade 3 and Brigade Major of an Independent Air Defence Brigade, Deputy Assistant Adjutant and Quarter Master General of an Infantry Brigade, and Senior Instructor Gunnery in the School of Artillery. Under Blue Helmet, he took part in peacekeeping operations as a Contingent Member in Ivory Coast (UNOCI) and as a Military Analyst in the Joint Mission Analysis Center in Mali (MINUSMA). Apart from mandatory courses, the researcher has attended the Missile Battery Commander Course in China and the Certificate on Terrorism Studies from the University of St Andrews, Scotland. He is a graduate of Defence Services Command and Staff College, Mirpur and Artillery Center and School, Halishahar under the Bangladesh University of Professionals (BUP). Presently, the officer is serving in National Defence College as a Senior Research Fellow.

NDC JOURNAL

Security Through Knowledge

NDC Journal
National Defence College
Mirpur Cantonment, Dhaka-1216
Bangladesh
(ISSN: 1683-8475)

NDC JOURNAL

NDC Journal is a professional journal of the National Defence College, Bangladesh. It is published twice a year by the College.

Its goal is to provide a platform for exchange of knowledge, experience, ideas, information and data on all aspects related to National Security and Development. The primary emphasis of the journal is the publication of empirically based, policy-oriented articles which can attract the attention of policy-makers both at government and private level, security and development experts, academicians, researchers and the members of public in general.

The Editorial Board welcomes original works analyzing, development and security issues. The articles, as desired, should have a strong emphasis on the policy implications flowing from the research.

Please visit our NDC E-JOURNAL at https://ndcjournal.ndc.gov.bd/ndcj/

National Defence College, Mirpur Cantonment, Dhaka-1216
Tel : 88 02 9003087, Fax : 88 02 8034715
e-mail: ndcbangladesh@ndc.gov.bd
Website : http://www.ndc.gov.bd